ALGEBRAS AND THEIR ARITHMETICS

By

LEONARD EUGENE DICKSON

Professor of Mathematics, University of Chicago

REPRINT OF THE 1923 EDITION

NEW YORK

G. E. STECHERT & CO.

1938

Published July 1923

PREFACE

The chief purpose of this book is the development for the first time of a general theory of the arithmetics of algebras, which furnishes a direct generalization of the classic theory of algebraic numbers. The book should appeal not merely to those interested in either algebra or the theory of numbers, but also to those interested in the foundations of mathematics. Just as the final stage in the evolution of number was reached with the introduction of hypercomplex numbers (which make up a linear algebra), so also in arithmetic, which began with integers and was greatly enriched by the introduction of integral algebraic numbers, the final stage of its development is reached in the present new theory of arithmetics of linear algebras.

Since the book has interest for wide classes of readers, no effort has been spared in making the presentation clear and strictly elementary, requiring on the part of the reader merely an acquaintance with the simpler parts of a first course in the theory of equations. Each definition is illustrated by a simple example. Each chapter has an appropriate introduction and summary.

The author's earlier brief book, *Linear Algebras* (Cambridge University Press, 1914), restricted attention to complex algebras. But the new theory of arithmetics of algebras is based on the theory of algebras over a general field. The latter theory was first presented by Wedderburn in his memoir in the *Proceedings of the London Mathematical Society* for 1907. The proofs of

some of his leading theorems were exceedingly complicated and obscured by the identification of algebras having the same units but with co-ordinates in different fields. Scorza in his book, *Corpi Numerici e Algebre* (Messina [1921], ix+462 pp.), gave a simpler proof of the theorem on the structure of simple algebras, but omitted the most important results on division algebras as well as the principal theorem on linear algebras. An outline of a new simpler proof of that theorem was placed at the disposal of the author by Wedderburn, with whom the author has been in constant correspondence while writing this book, and who made numerous valuable suggestions after reading the part of the manuscript which deals with the algebraic theory. However, many of the proofs due essentially to Wedderburn have been recast materially. Known theorems on the rank equations of complex algebras have been extended by the author to algebras over any field. The division algebras discovered by him in 1906 are treated more simply than heretofore.

Scorza's book has been of material assistance to the author although the present exposition of the algebraic part differs in many important respects from that by Scorza and from that in the author's earlier book.

But the chief obligations of the author are due to Wedderburn, both for his invention of the general theory of algebras and for his cordial co-operation in the present attempt to perfect and simplify that theory and to render it readily accessible to general readers.

The theory of arithmetics of algebras has been surprisingly slow in its evolution. Quite naturally the arithmetic of quaternions received attention first;

the initial theory presented by Lipschitz in his book of 1886 was extremely complicated, while a successful theory was first obtained by Hurwitz in his memoir of 1896 (and book of 1919). Du Pasquier, a pupil of Hurwitz, has proposed in numerous memoirs a definition of integral elements of any rational algebra which is either vacuous or leads to insurmountable difficulties discussed in this book. Adopting a new definition, the author develops at length a far-reaching general theory whose richness and simplicity mark it as the proper generalization of the theory of algebraic numbers to the arithmetic of any rational algebra.

Acknowledgments are due to Professor Moore, the chairman of the Editorial Committee of the University of Chicago Science Series, for valuable suggestions both on the manuscript and on the proofsheets of the chapter on arithmetics.

L. E. DICKSON

UNIVERSITY OF CHICAGO
June, 1923

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION, DEFINITIONS OF ALGEBRAS, ILLUSTRATIONS

The co-ordinates of the numbers of an algebra may be ordinary complex numbers, real numbers, rational numbers, or numbers of any field. By employing a general field of reference, we shall be able to treat together complex algebras, real algebras, rational algebras, etc., which were discussed separately in the early literature.

We shall give a brief introduction to matrices, partly to provide an excellent example of algebras, but mainly because matrices play a specially important rôle in the theory of algebras.

1. **Fields of complex numbers.** If a and b are real numbers and if i denotes $\sqrt{-1}$, then $a+bi$ is called a complex number.

A set of complex numbers will be called a *field* if the sum, difference, product, and quotient (the divisor not being zero) of any two equal or distinct numbers of the set are themselves numbers belonging to the set.

For example, all complex numbers form a field C. Again, all real numbers form a field $\mathfrak{R}$. Likewise, the set of all rational numbers is a field R. But the set of all integers (i.e., positive and negative whole numbers and zero) is not a field, since the quotient of two integers is not always an integer.

Next, let α be an algebraic number, i.e., a root of an algebraic equation whose coefficients are all rational numbers. Then the set of all rational functions of α

with rational coefficients evidently satisfies all the requirements made in the foregoing definition of a field, and is called an algebraic number field.

The latter field is denoted by $R(a)$ and is said to be an *extension* of the field R of all rational numbers by the *adjunction* of a. It has R as a *sub-field*.

Similarly, the field C of all complex numbers is the extension $\Re(i)$ of the field $\Re$ of all real numbers by the adjunction of i.

All of the fields mentioned above are sub-fields of C. For such fields the reader is familiar with the algebraic theorems which will be needed in the development of the theory of linear algebras. However, that theory will be so formulated that it is valid not merely for a sub-field of C, but also for an arbitrary field (occasionally with a restriction expressly stated). Mature readers who desire to interpret the theory of algebras as applying to an arbitrary field are advised to read first chapter xi, which presents the necessary material concerning general fields.

2. Linear transformations. The pair of equations

$$t: \quad x=a\xi+b\eta, \quad y=c\xi+d\eta, \quad D=\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0,$$

with coefficients in any field F, is said to define a linear transformation t, of determinant D, from the initial independent variables x, y to the new independent variables ξ, η.

Consider a second linear transformation

$$\tau: \quad \xi=\alpha X+\beta Y, \quad \eta=\gamma X+\delta Y, \quad \Delta=\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \neq 0,$$

from the variables ξ, η to the final independent variables X, Y. If we eliminate ξ and η between our four equations, we obtain the equations

$$t_1: \qquad x=a_1X+b_1Y, \qquad y=c_1X+d_1Y,$$

in which we have employed the following abbreviations:

$$(1) \quad a_1=a\alpha+b\gamma, \quad b_1=a\beta+b\delta, \quad c_1=c\alpha+d\gamma, \quad d_1=c\beta+d\delta,$$

whence

$$(2) \qquad \begin{vmatrix} a_1 & b_1 \\ c_1 & d_1 \end{vmatrix} = D\Delta \neq 0.$$

Instead of passing from the initial variables x, y to the intermediate variables ξ, η by means of transformation t, and afterward passing from ξ, η to the final variables X, Y by means of transformation τ, we may evidently pass directly from the initial variables x, y to the final variables X, Y by means of the single transformation t_1. We shall call t_1 the *product* of t and τ taken in that order and write $t_1=t\tau$. This technical term "product" has the sense of resultant or compound. Similarly, we may travel from a point A to a point B, and later from B to C, or we may make the through journey from A to C without stopping at B.

By solving the equations which define t, we get

$$\xi=\frac{d}{D}x-\frac{b}{D}y, \qquad \eta=\frac{-c}{D}x+\frac{a}{D}y.$$

If we continue to regard x, y as the initial variables and ξ, η as the new variables, we still have the same transformation t expressed in another form. But if we regard ξ, η as the initial variables and x, y as the new variables,

we obtain another transformation called the *inverse* of t and denoted by t^{-1}. It will prove convenient to write X, Y for x, y; then

$$t^{-1}: \qquad \xi=\frac{d}{D}X-\frac{b}{D}Y, \qquad \eta=\frac{-c}{D}X+\frac{a}{D}Y.$$

Eliminating ξ and η between the four equations defining t and t^{-1}, we find that the product tt^{-1} is

$$I: \qquad x=X, \qquad y=Y,$$

which is called the *identity transformation* I. As would be anticipated, also $t^{-1}t=I$.

While $t^{-1}t=tt^{-1}$, usually two transformations t and τ are not *commutative*, $t\tau\neq\tau t$, since the sums in (1) are usually altered when the Roman and Greek letters are interchanged. However, the associative law

$$(t\tau)T=t(\tau T)$$

holds for any three transformations, so that we may write $t\tau T$ without ambiguity. For, if we employ the foregoing general transformations t and τ, and

$$T: \qquad X=Au+Bv, \qquad Y=Cu+Dv,$$

we see that $(t\tau)T$ is found by eliminating first ξ, η and then X, Y between the six equations for t, τ, T, while $t(\tau T)$ is obtained by eliminating first X, Y and then ξ, η between the same equations. Since the same four variables are eliminated in each case, we must evidently obtain the same final two equations expressing x and y in terms of u and v.

The foregoing definitions and proofs apply at once to linear transformations on any number p of variables:

$$A: \quad \begin{aligned} x_1 &= a_{11}\xi_1 + a_{12}\xi_2 + \ldots + a_{1p}\xi_p, \\ &\ldots\ldots\ldots\ldots\ldots \\ x_p &= a_{p1}\xi_1 + a_{p2}\xi_2 + \ldots + a_{pp}\xi_p, \end{aligned}$$

except that the equations of the inverse A^{-1} are now more complicated (§ 3).

3. **Matrices.** A linear transformation is fully defined by its coefficients, while it is immaterial what letters are used for the initial and the final variables. For example, when we wrote the equations for t^{-1} in § 2, we replaced the letters x, y which were first employed to designate the new variables by other letters X, Y.

Hence the transformations t, τ, and A in § 2 are fully determined by their matrices:

$$m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \mu = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad \begin{pmatrix} a_{11}, & a_{12}, \ldots, & a_{1p} \\ \ldots & \ldots & \ldots \\ a_{p1}, & a_{p2}, \ldots, & a_{pp} \end{pmatrix},$$

the last having p rows with p elements in each row. Such a p-rowed square *matrix* is an ordered set of p^2 elements each occupying its proper position in the symbol of the matrix. The idea is the same as in the notation for a point (x, y) of a plane or for a point (x, y, z) in space, except that these one-rowed matrices are not square matrices. The matrix

$$m\mu = \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix}$$

of the transformation $t_1 = t\tau$ is called the *product* of the matrices m and μ of the transformations t and τ. Hence the element in the ith row and jth column of the product of two matrices is the sum of the products of the succes-

sive elements of the ith row of the first matrix by the corresponding elements of the jth column of the second matrix.

For example, the element $a\beta+b\delta$ in the first row and second column of $m\mu$ is found by multiplying the elements a, b of the first row of m by the elements β, δ, respectively, of the second column of μ, and adding the two products.

The determinants D and Δ of the transformations t and τ are called the determinants of their matrices m and μ. By (2), the determinant of their product $m\mu$ is equal to the product $D\Delta$ of their determinants.

We shall call the matrices m and μ *equal*, and write $m=\mu$, if and only if their corresponding elements are equal:

$$a=\alpha, \quad b=\beta, \quad c=\gamma, \quad d=\delta.$$

In § 2, we employed only transformations whose determinants are not zero. This restriction is necessary if we desire that the initial variables shall be independent, as well as the new variables. For, if $D=0$ and $a\neq 0$ in t, then $y=a^{-1}cx$. But let us employ also *degenerate transformations* (of determinant zero), i.e., linear relations between two sets of variables, the variables in one or both sets being dependent. Then the product of any two linear transformations, whether degenerate or not, is found as before by elimination of the intermediate set of variables. Hence we may apply our rule of multiplication to any two matrices, and conclude from § 2 that this multiplication obeys the associative law.

In particular, $mI = Im = m$ for every two-rowed matrix m if

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is the *identity matrix*, or *unit matrix*. If the determinant D of m is not zero, m has the *inverse*

$$m^{-1} = \begin{pmatrix} d/D & -b/D \\ -c/D & a/D \end{pmatrix}, \qquad m^{-1}m = mm^{-1} = I.$$

The corresponding matrix without the denominators D is called the *adjoint* of m and designated by "adj. m."

If m is a p-rowed square matrix, the element in the ith row and jth column of its adjoint is the cofactor (signed minor) of the element in the jth row and ith column of the determinant D of m. In case $D \neq 0$, the element in the ith row and jth column of the inverse m^{-1} of m is the quotient of that cofactor by D.

Given two matrices m and μ such that the determinant $|m|$ of m is not zero, we can find one and only one matrix $x = m^{-1}\mu$ such that $mx = \mu$, and also one and only one matrix $y = \mu m^{-1}$ such that $ym = \mu$.

But if $|m| = 0$, there is no matrix x for which $mx = I$, since this would imply $0 \cdot |x| = 1$. Likewise there is no matrix y for which $ym = I$.

Hence each of the two kinds of division by m is always possible and unique if and only if $|m| \neq 0$.

The sum of the foregoing two-rowed matrices m and μ is defined to be

$$m + \mu = \begin{pmatrix} a+\alpha & b+\beta \\ c+\gamma & d+\delta \end{pmatrix}.$$

Hence the matrix all of whose elements are zero plays the rôle of zero in addition.

Denote by S_e the *scalar matrix* whose diagonal elements are all e and whose remaining elements are all zero; if there are only two rows,

$$S_e=\begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix}.$$

If a and b are any two numbers of the field F,

$$S_a+S_b=S_{a+b}, \qquad S_aS_b=S_{ab}.$$

Hence there is evidently a one-to-one correspondence between the scalar matrices S_e and the numbers e of the field F such that this correspondence is preserved under both addition and multiplication. In other words, the set of all scalar matrices is a field simply isomorphic with F. Moreover,

$$S_em=mS_e=\begin{pmatrix} ea & eb \\ ec & ed \end{pmatrix}, \qquad m\equiv\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Hence from any relation between matrices, some of which are scalar, we obtain a true relation if we replace each scalar matrix S_e by the number e and make the following definitions:

$$em=me=\begin{pmatrix} ea & eb \\ ec & ed \end{pmatrix}, \qquad e+m=m+e=\begin{pmatrix} a+e & b \\ c & d+e \end{pmatrix}.$$

The first relation defines the *scalar product* of a number e and a matrix m to be the matrix each of whose elements is the product of e by the corresponding element of m. In particular, $eI=Ie=S_e$. Use is rarely made of the notation $e+m$, which is generally written $eI+m$.

If m is a matrix whose determinant D is not zero, then adj. $m = Dm^{-1}$ by the foregoing definitions. Hence the product of m and adj. m in either order is DI. This result holds true also if $D = 0$.

Important theorems on matrices are proved in chapter vii.

4. Definition of an algebra over any field. According to the definition to be given, the set of all complex numbers $a+bi$ is an algebra over the field of all real numbers. Again, the set of all p-rowed square matrices with elements in any field F is an algebra over F (§ 8). In this algebra, multiplication is usually not commutative, while division may fail.

The foregoing discussion of matrices and operations on them provides an excellent concrete introduction to the following abstract definition of algebras.

The elements of an algebra will be denoted by small Roman letters, while the numbers of a field F will be denoted by small Greek letters.

An *algebra* A over a field F is a system consisting of a set S of two or more elements $a, b, c, \ldots$ and three operations $\oplus$, $\odot$, and $\bigcirc$, of the types specified below, which satisfy postulates I–V. The operation $\oplus$, called *addition*, and the operation $\odot$, called *multiplication*, may be performed upon any two (equal or distinct) elements a and b of S, taken in that order, to produce unique elements $a \oplus b$ and $a \odot b$ of S, which are called the *sum* and *product* of a and b, respectively. The operation $\bigcirc$, called *scalar multiplication*, may be performed upon any number α of F and any element a of S, or upon a and α, to produce a unique element $\alpha \bigcirc a$ or $a \bigcirc \alpha$ of S, called a *scalar product.*

For simplicity we shall write $a+b$ for $a \oplus b$, ab for $a \odot b$, aa for $a \bigcirc a$, and aa for $a \bigcirc a$, and we shall speak of the elements of S as elements of A.

We assume that addition is commutative and associative:

I. $\quad a+b=b+a, \qquad (a+b)+c=a+(b+c),$

whence the sum $a_1+ \ldots . +a_t$ of $a_1, \ldots . , a_t$ is defined without ambiguity.

For scalar multiplication, we assume that

II. $\quad \alpha a=a\alpha, \qquad \alpha(\beta a)=(\alpha\beta)a, \qquad (\alpha a)(\beta b)=(\alpha\beta)(ab),$

III. $\quad (\alpha+\beta)a=\alpha a+\beta a, \qquad \alpha(a+b)=\alpha a+\alpha b.$

Multiplication is assumed to be distributive with respect to addition:

IV. $\quad (a+b)c=ac+bc, \qquad c(a+b)=ca+cb.$

But multiplication need not be either commutative or associative. However, beginning with chapter iv, we shall assume the associative law $(ab)c=a(bc)$, and then call the algebra *associative.*

The final assumption serves to exclude algebras of infinite order:

V. The algebra A has a finite basis.

This shall mean that A contains a finite number of elements $v_1, \ldots . , v_m$ such that every element of A can be expressed as a sum $a_1v_1+ \ldots . +a_mv_m$ of scalar products of $v_1, \ldots . , v_m$ by numbers $a_1, \ldots . , a_m$ of F.

The reader who desires to avoid technical discussions may omit the proof below that postulates I–V imply property VI, and at once assume VI instead of V.

VI. The algebra A contains elements $u_1, \ldots, u_n$ such that every element x of A can be expressed in one and *only one* way in the form

$$x=\xi_1 u_1+\ldots+\xi_n u_n, \tag{3}$$

where $\xi_1, \ldots, \xi_n$ are numbers of the field F.

This implies that if x is equal to

$$y=\eta_1 u_1+\ldots+\eta_n u_n, \tag{4}$$

then $\xi_1=\eta_1, \ldots, \xi_n=\eta_n$. Adding the n terms of x to those of y, and applying I and III_1, we get

$$x+y=(\xi_1+\eta_1)u_1+\ldots+(\xi_n+\eta_n)u_n. \tag{5}$$

An element z such that $x+z=x$ for every x in A is called a *zero* element of A. Comparing (3) with (5), we see that $x+y=x$ if and only if $\eta_1=0, \ldots, \eta_n=0$. Hence the unique zero element is

$$z=0\cdot u_1+\ldots+0\cdot u_n.$$

It will be denoted by 0 in the later sections.

We shall now deduce certain results from I–V which will enable us to prove VI. We first prove that $1\cdot x=x$ for every x in A. By V, $x=\Sigma a_i v_i$. Then, by III_2 and II_2,

$$1\cdot x=\Sigma 1\cdot(a_i v_i)=\Sigma(1\cdot a_i)v_i=\Sigma a_i v_i=x.$$

Write $z_i=0\cdot v_i$ for $i=1, \ldots, m$, and $z=z_1+\ldots+z_m$. By III_1 for $\alpha=0, \beta=1$, we have $a=0\cdot a+a$. Take $a=a_i v_i$ and note that, by II_2,

$$0\cdot a_i v_i=(0\cdot a_i)v_i=0\cdot v_i=z_i. \tag{6}$$

Hence $a_i v_i=z_i+a_i v_i$. Summing for $i=1, \ldots, m$, we get $x=z+x$. Suppose that also $x=w+x$ for every x in

A, whence $z=w+z$. By the former result with $x=w$, we have $w=z+w$, whence $w=w+z$ by I. Hence $w=z$. Hence A contains a unique *zero* element z such that $x=z+x$ for every x in A.

By summing (6) for $i=1, \ldots, m$, and applying III_2, we get $0 \cdot x=z$ for every x in A. Next, by II_3,

$$z_i x=(0 \cdot v_i)x=(0 \cdot v_i)(1 \cdot x)=(0 \cdot 1)(v_i x)=0(v_i x)=z .$$

Summing for $i=1, \ldots, m$, and noting that $z+z=z$, we get $zx=z$. Similarly, $xz_i=z$, whence $xz=z$. For any number ρ in F,

$$\rho z_i=\rho(0 \cdot v_i)=(\rho \cdot 0)v_i=0 \cdot v_i=z_i , \qquad \rho z=z .$$

Define $-x$ to be the scalar product of -1 by x. By III_1 for $\alpha=1$, $\beta=-1$, we get $z=\alpha+(-\alpha)$.

Define $x-y$ to mean $x+(-y)$ and call it the result d of subtracting y from x. By adding y to each member of $x-y=d$, and applying the preceding conclusion, we get

$$x-y+y=x+z=x=d+y .$$

Conversely, if $x=d+y$, add $-y$ to each member; then

$$x-y=d+y+(-y)=d+z=d .$$

Hence any term of one member of an equation may be carried to the other member after changing the sign of the term.

We are now in a position to prove VI. Either the v_i in V will serve as the desired u_i, or there exists at least one relation $\Sigma\gamma_i v_i=\Sigma\beta_i v_i$ in which $\gamma_i \neq \beta_i$ for some value $\leqq m$ of i. Since we may permute the v_i, we may assume without loss of generality that $\gamma_m \neq \beta_m$.

Then there exists a number ρ of the field F such that $\rho(\beta_m - \gamma_m) = 1$. We transpose terms, apply III_1, multiply on the left by ρ, apply II_4, and get

$$\sum_{j=1}^{m-1} \rho(\gamma_j - \beta_j) \cdot v_j = v_m .$$

If $^*m > 1$, we may therefore eliminate v_m from $\Sigma a_i v_i$ and obtain a linear function of $v_1, \ldots, v_{m-1}$ with coefficients δ_i in F. If two such linear functions are equal without being identical, a repetition of the argument shows that we may eliminate one of $v_1, \ldots, v_{m-1}$ from $\Sigma \delta_i v_i$. Evidently this process ultimately leads to a set of elements $u_1, \ldots, u_n$ having property VI.

This definition of an algebra, with V replaced by the much stronger assumption VI, is due to G. Scorza.† However essentially the same definition of an algebra over the field of real numbers had been given in *Encyclopédie des Sciences Mathématiques*, Tome I, Volume I (1908), pages 369–78.

5. Linear dependence with respect to a field. Elements $e_1, \ldots, e_k$ of an algebra A over F are said to be *linearly dependent* with respect to F if there exist numbers $a_1, \ldots, a_k$, not all zero, of F such that $a_1 e_1 + \ldots + a_k e_k = 0$. If no such numbers a_i exist, the e_i are called *linearly independent* with respect to F. An example is given in § 8.

* If $m = 1$, we proved that $z = v_1$. Hence, by V, every element of A is the form $a_1 v_1 = a_1 z = z$, whereas A was assumed to contain at least two elements. This contradiction shows that v_1 in V serves as u_1 in VI and that $n = 1$.

† *Corpi Numerici e Algebre* (Messina, 1921), p. 180; *Rendiconti Circolo Matematico di Palermo*, XLV (1921), 7.

THEOREM. If $u_1, \ldots, u_n$ *are linearly independent with respect to a field* F, *the* n *linear functions*

$$(7) \quad l_i = \beta_{i1}u_1 + \ldots + \beta_{in}u_n \qquad (i = 1, \ldots, n),$$

with coefficients in F, *are linearly independent or dependent according as the determinant* $\beta = |\beta_{ij}|$ *is not zero or is zero in* F.

For, if $a_1, \ldots, a_n$ are numbers of F,

$$\sum_{i=1}^{n} a_i l_i = \sum_{i=1}^{n} a_i \beta_{i1} u_1 + \ldots + \sum_{i=1}^{n} a_i \beta_{in} u_n$$

is zero if and only if

$$(8) \qquad \sum_{i=1}^{n} \beta_{i1} a_i = 0, \ldots, \sum_{i=1}^{n} \beta_{in} a_i = 0.$$

The determinant of the coefficients of $a_1, \ldots, a_n$ in equations (8) is β. Hence the ordinary rule for solving linear equations by determinants gives $\beta a_1 = 0, \ldots, \beta a_n = 0$. If $\beta \neq 0$, $a_1, \ldots, a_n$ are all zero, so that $l_1, \ldots, l_n$ are linearly independent. But if $\beta = 0$, the n linear homogeneous equations (8) have solutions* $a_1, \ldots, a_n$, not all zero, whence $l_1, \ldots, l_n$ are linearly dependent.

6. Order and basal units of an algebra. In view of VI, in § 4, the algebra A over F is said to be of *order* n, and $u_1, \ldots, u_n$ are said to form a set of n *basal units* of A.

* Dickson *First Course in the Theory of Equations* (1922), p. 119.

The last name is given also to any set of n linearly independent linear functions (7) of $u_1, \ldots, u_n$ with coefficients in F. Then the determinant of those coefficients is not zero, and (7) can be solved for $u_1, \ldots, u_n$ in terms of $l_1, \ldots, l_n$. Hence every element $\Sigma a_i u_i$ of A can be expressed as a linear function of $l_1, \ldots, l_n$ with coefficients in F.

This replacement of one set of basal units $u_1, \ldots, u_n$ by another set $l_1, \ldots, l_n$ is called a *transformation of units*. The work will be carried out in full detail in § 61.

THEOREM. *Any $n+1$ elements of A are linearly dependent with respect to F.*

For, $l_1, \ldots, l_{n+1}$ are evidently dependent if $l_1, \ldots, l_n$ are. In the contrary case, we saw that l_{n+1} can be expressed as a linear function of $l_1, \ldots, l_n$ with coefficients in F, so that $l_1, \ldots, l_{n+1}$ are dependent.

7. Modulus. An algebra A may have an element e, called a *modulus* (or principal unit), such that $ex = xe = x$ for every element x of A. For example, the unit matrix I (§ 3) is a modulus for all square matrices having the same number of rows as I.

If there were a modulus s other than e, then $se = e$, while $se = s$ by taking $x = s$ in the earlier relations. Hence $s = e$, so that there is at most one modulus. It is often designated by 1 since it plays the rôle of unity in multiplication.

If an algebra A over F has the modulus e, the totality of elements ae, where a belongs to F, constitutes an algebra of order 1. Since $ae + a'e = (a+a')e$, $ae \cdot a'e = aa'e$, this algebra of order 1 is called simply isomorphic with the field F.

8. Examples of associative algebras. The totality of p-rowed square matrices with elements in any field F is an associative algebra of order p^2 over F, when addition, multiplication, and scalar multiplication are defined as in § 3. We may choose as a set of p^2 basal units $e_{ij}(i, j=1, \ldots, p)$, where e_{ij} denotes the matrix whose elements are all zero except that in the ith row and jth column, while that element is 1. For $p=2$,

$$e_{11}=\begin{pmatrix}1&0\\0&0\end{pmatrix},\quad e_{12}=\begin{pmatrix}0&1\\0&0\end{pmatrix},\quad e_{21}=\begin{pmatrix}0&0\\1&0\end{pmatrix},\quad e_{22}=\begin{pmatrix}0&0\\0&1\end{pmatrix}.$$

Then

$$\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}=\alpha e_{11}+\beta e_{12}+\gamma e_{21}+\delta e_{22}$$

is zero only when $\alpha=\beta=\gamma=\delta=0$, whence the four e_{ij} are linearly independent with respect to F (cf. § 9, end).

Second, the field C of all complex numbers $\xi+\eta i$ may be regarded as an algebra of order 2 with the basal units $u_1=1$, $u_2=i$, over the field F of all real numbers. For, the assumptions I–IV are satisfied when the Roman letters denote any numbers of the field C and the Greek letters denote any real numbers.

Third, any field F may be regarded as an algebra, over F, of order 1, whose basal unit is 1 (or any chosen number $\neq 0$ of F).

9. An algebra in terms of its units. Choose any set of basal units $u_1, \ldots, u_n$ of an algebra A of order n over the field F. By VI, any elements x and y of A can be expressed in one and but one way in the respective forms

$$(9) \qquad x=\sum_{i=1}^{n}\xi_i u_i, \qquad y=\sum_{i=1}^{n}\eta_i u_i,$$

where $\xi_1, \ldots, \xi_n$ are numbers of F called the *coordinates* of x (with respect to the chosen units). By § 4,

$$(10) \quad x+y=\sum_{i=1}^{n}(\xi_i+\eta_i)u_i, \qquad x-y=\sum_{i=1}^{n}(\xi_i-\eta_i)u_i.$$

By IV and II_3, we have

$$(11) \qquad xy=\sum_{i,j=1}^{n}\xi_i\eta_j \cdot u_i u_j.$$

By VI,

$$(12) \qquad u_i u_j=\sum_{k=1}^{n}\gamma_{ijk}u_k \qquad (i,j=1, \ldots, n),$$

where the n^3 numbers γ_{ijk} belong to F and are called the *constants of multiplication* of the algebra A (with respect to the units $u_1, \ldots, u_n$). The n^2 relations (12) are said to give the *table* of multiplication* of A (with respect to the units $u_1, \ldots, u_n$).

From (11) and (12), we get, by III_2 and II_2,

$$(13) \qquad xy=\sum_{i,j,k=1}^{n}\xi_i\eta_j\gamma_{ijk} \cdot u_k.$$

From (9_1) we obtain, by III, II_2, and II_1,

$$(14) \qquad \rho x=x\rho=\sum_{i=1}^{n}(\rho\xi_i)u_i \qquad (\rho \text{ in } F).$$

* We may use an actual table as in § 25.

The set of elements (9_1) form an algebra A over F with respect to addition, multiplication, and scalar multiplication, defined by (10_1), (13), and (14), respectively, since postulates I–V of § 4 are easily seen to be satisfied. Hence we may operate concretely on the elements of an algebra by the rules of this section without recourse to § 4.

To illustrate these rules for the algebra of all two-rowed square matrices with elements in F, we write the matrices m, μ, $m+\mu$, and $m\mu$ of § 3 in terms of the basal units e_{ij} defined in § 8 and obtain

$$m = ae_{11}+be_{12}+ce_{21}+de_{22},$$
$$\mu = \alpha e_{11}+\beta e_{12}+\gamma e_{21}+\delta e_{22},$$
$$m+\mu = (a+\alpha)e_{11}+(b+\beta)e_{12}+(c+\gamma)e_{21}+(d+\delta)e_{22},$$
$$m\mu = (a\alpha+b\gamma)e_{11}+(a\beta+b\delta)e_{12}+(c\alpha+d\gamma)e_{21}+(c\beta+d\delta)e_{22}.$$

The last equation may also be verified by means of the following table of multiplication of the units:

$$(15) \qquad e_{ij}e_{jk} = e_{ik}, \qquad e_{ij}e_{lk} = 0 \qquad (l \neq j).$$

10. New form of the foregoing matric algebra. Consider the complex matric algebra of all two-rowed square matrices whose elements are complex numbers. We employed above the set of basal units e_{11}, e_{12}, e_{21}, e_{22}. Then $e_{11}+e_{22}$ is the unit matrix or modulus, which will here be designated by 1.

We shall introduce the new set of basal units,

$$(16) \quad 1 = e_{11}+e_{22}, \qquad u_1 = \sqrt{-a}(e_{11}-e_{22}), \qquad u_2 = e_{12}-\beta e_{21},$$
$$u_3 = \sqrt{-a}(e_{12}+\beta e_{21}),$$

where $\alpha \neq 0$, $\beta \neq 0$. We have

$$(17) \qquad u_1 = \begin{pmatrix} \sqrt{-\alpha} & 0 \\ 0 & -\sqrt{-\alpha} \end{pmatrix}, \qquad u_2 = \begin{pmatrix} 0 & 1 \\ -\beta & 0 \end{pmatrix},$$

$$u_3 = \begin{pmatrix} 0 & \sqrt{-\alpha} \\ \beta\sqrt{-\alpha} & 0 \end{pmatrix}.$$

By actual multiplication of matrices we readily get

$$u_1^2 = \begin{pmatrix} -\alpha & 0 \\ 0 & -\alpha \end{pmatrix} = -\alpha, \quad u_2^2 = -\beta, \quad u_3^2 = -\alpha\beta, \quad u_1 u_2 = u_3.$$

Since matric multiplication is associative, we get

$$\begin{aligned} u_1 u_3 &= u_1 u_1 u_2 = -\alpha u_2, & u_3 u_2 &= u_1 u_2 u_2 = -\beta u_1, \\ -\alpha\beta u_2 &= u_3^2 u_2 = u_3(-\beta u_1) \quad \text{or} & u_3 u_1 &= \alpha u_2, \\ \alpha u_2 u_1 &= u_3 u_1 \cdot u_1 = u_3(-\alpha), & u_2 u_3 &= -u_1 \cdot u_2 u_1 = \beta u_1. \end{aligned}$$

Hence the multiplication table of the units 1, u_1, u_2, u_3 is

$$(18) \quad \begin{cases} u_1^2 = -\alpha, \ u_2^2 = -\beta, \ u_3^2 = -\alpha\beta, \ u_1 u_2 = u_3, \ u_2 u_1 = -u_3, \\ u_1 u_3 = -\alpha u_2, \ u_3 u_1 = \alpha u_2, \ u_2 u_3 = \beta u_1, \ u_3 u_2 = -\beta u_1, \\ 1 \cdot u_r = u_r \cdot 1 = u_r \qquad (r = 1, 2, 3). \end{cases}$$

The linear combinations of 1, u_1, u_2, u_3 with complex coefficients constitute an algebra which is merely another form of the complex matric algebra with the units e_{11}, e_{12}, e_{21}, e_{22}.

But if we restrict the co-ordinates of $\sigma + \xi u_1 + \eta u_2 + \zeta u_3$ to be numbers of any field F which contains α and β, we obtain an associative algebra over F.

11. Quaternions. If in (18) we take $\alpha = \beta = 1$ and write i, j, k for u_1, u_2, u_3, we obtain the multiplication table

$$(19) \quad \begin{cases} i^2 = j^2 = k^2 = -1, \quad ij = k, \quad ji = -k, \quad ki = j, \\ ik = -j, \ jk = i, \ kj = -i, \ 1i = i1 = i, \text{ etc.} \end{cases}$$

of the basal units of *quaternions* $q=\sigma+\xi i+\eta j+\zeta k$. The totality of elements q with $\sigma, \ldots, \zeta$ in any field F is the associative algebra of quaternions over F. When $\sigma, \ldots, \zeta$ are all complex, real, or rational, q is called a complex, real, or rational quaternion, respectively.

Define the *conjugate* q' and *norm* $N(q)$ of q to be

$$q'=\sigma-\xi i-\eta j-\zeta k, \qquad N(q)=qq'=q'q=\sigma^2+\xi^2+\eta^2+\zeta^2.$$

The conjugate of a product qq_1 is readily verified to be equal to the product $q_1'q'$ of the conjugates in reverse order. Thus $N(qq_1)=qq_1q_1'q'$. Since q_1q_1' is a number $N(q_1)$ of F it may be moved to the right of q'. Hence $N(qq_1)=N(q)\cdot N(q_1)$. In other words the norm of a product of any two quaternions is equal to the product of their norms.

Let F be a field composed only of real numbers. Then a sum of squares is zero only when each square is zero. Thus if $q\neq 0$, then $N(q)\neq 0$ and q has the inverse

$$q^{-1}=\frac{1}{N(q)}q'.$$

Hence, if $q\neq 0$, $qx=q_1$ has the unique solution $x=q^{-1}q_1$, and $yq=q_1$ has the unique solution $y=q_1q^{-1}$. Thus each of the two kinds of division by $q\neq 0$ is always possible and unique in the algebra of quaternions over any real field. In particular, a product of two real quaternions is zero only when one factor is zero.

12. Equivalent and reciprocal algebras. Two algebras A and A' over the same field F are called *equivalent* (or *simply isomorphic*) if it is possible to establish between their elements a (1, 1) correspondence such that

if any elements x and y of A correspond to the elements x' and y' of A', also the elements $x+y$, xy and ax of A correspond to the elements $x'+y'$, $x'y'$ and ax' of A', for every number a of F.

Equivalent algebras have the same order, and their elements zero correspond. If one of two equivalent algebras has a modulus, so does the other, and the moduli correspond.

Any algebra A over F is equivalent to itself under any linear transformation of units with coefficients in F (§ 6).

For example, if we take $\alpha=\beta=1$ in § 10, we see that the algebra of all two-rowed matrices whose elements are complex numbers is equivalent, by means of the transformation (16) on the units, to the algebra of all complex quaternions. But since that transformation has imaginary coefficients, it does not set up a correspondence between real matrices and real quaternions. The two real algebras are in fact not equivalent; various products $e_{r1}e_{2s}(r=1, 2;\ s=1, 2)$ of real matrices are zero, although each factor is not zero, while the product of two real quaternions, each not zero, is never zero.

Two algebras A and A' over F are called *reciprocal* if it is possible to establish a (1, 1) correspondence between their elements such that $x+y$, xy, ax now correspond to $x'+y'$, $y'x'$, ax'.

If in the multiplication table (12) of the units of an algebra A over F, we replace each product u_iu_j by $u'_ju'_i$, we obtain the multiplication table of the units $u'_1, \ldots, u'_n$ of an algebra A' over F which is reciprocal to A. For example, from (15) we get

$$e'_{jk}e'_{ij}=e'_{ik}, \qquad e'_{lk}e'_{ij}=0 \qquad (l\neq j).$$

From these relations we obtain again (15), aside from the lettering of the subscripts, if we write e_{rs} for e'_{sr}, i.e., if we interchange the rows and columns of our matrices. Hence the algebra of all p-rowed matrices over F is self-reciprocal under the correspondence which interchanges the rows and columns of its matrices.

Two algebras which are either both equivalent or both reciprocal to the same algebra are equivalent to each other.

13. Second definition of an algebra. Each element $x=\Sigma\xi_i u_i$ of an algebra A over F, defined in § 4, has a unique set of co-ordinates $\xi_1, \ldots, \xi_n$ in F with respect to a chosen set of basal units $u_1, \ldots, u_n$. Hence with x may be associated a unique n-tuple* $[\xi_1, \ldots, \xi_n]$ of n ordered numbers of F. Using this n-tuple as a symbol for x, we may write equations (10_1), (13), (14) in the following form:

$$(20)\quad [\xi_1, \ldots, \xi_n]+[\eta_1, \ldots, \eta_n] = [\xi_1+\eta_1, \ldots, \xi_n+\eta_n],$$

$$(21)\quad [\xi_1, \ldots, \xi_n]\cdot[\eta_1, \ldots, \eta_n] = \left[\sum_{i,j=1}^{n}\xi_i\eta_j\gamma_{ij1}, \ldots, \sum_{i,j=1}^{n}\xi_i\eta_j\gamma_{ijn}\right],$$

$$(22)\quad \rho[\xi_1, \ldots, \xi_n]=[\xi_1, \ldots, \xi_n]\rho = [\rho\xi_1, \ldots, \rho\xi_n], \qquad \rho \text{ in } F.$$

These preliminaries suggest the following definition by W. R. Hamilton of an algebra A over F: Choose any n^3 constants γ_{ijk} of F, consider all *n-tuples* $[\xi_1, \ldots, \xi_n]$ of n ordered numbers of F, and define addition and

* For an algebra of two-rowed matrices, the numbers of each quadruple were written by twos in two rows.

multiplication of n-tuples by formulas (20) and (21), and scalar multiplication of a number of ρ of F and an n-tuple by formula (22). To pass to the definition in § 4, employ the particular n-tuples

$$(23)\quad u_1=[1, 0, \ldots, 0], \qquad u_2=[0, 1, 0, \ldots, 0], \ldots, \quad u_n=[0, \ldots, 0, 1]$$

as basal units. By (20) and (22), $[\xi_1, \ldots, \xi_n]=\xi_1u_1+\ldots+\xi_nu_n$. Then (20), (21), (22) take the form (10_1), (13), (14), and, as noted in § 9, all of the assumptions made in § 4 are satisfied. Hence an algebra of n-tuples is an algebra according to § 4 and conversely.

Hence there exists an algebra over F having as constants of multiplication any given n^3 numbers γ_{ijk} of F. The algebra will be associative if the γ's satisfy the conditions (§ 58) obtained from $(u_iu_j)u_k=u_i(u_ju_k)$.

14. Comparison of the two definitions of an algebra. Under the definition in § 4, an algebra over a field F is a system consisting of a set of wholly undefined elements and three undefined operations which satisfy five postulates.

Under Hamilton's definition in § 13, an algebra of order n over F is a system consisting of n^3 constants γ_{ijk} of F, a set of partially* defined elements $[\xi_1, \ldots, \xi_n]$, and three defined operations, while no postulates are imposed on the system other than that which partially determines the elements. This definition really implies a definite set (23) of basal units. A transformation of units leads to a new algebra (equivalent to the initial algebra) with new values for the n^3 constants γ_{ijk}.

* Each element is an n-tuple of numbers of F. In particular, if F is a finite field of order p, there are evidently exactly p^n elements.

But under the definition in § 4, no specific set of basal units is implied,* and we obtain the same algebra (not merely an equivalent one) when we make a transformation of units with coefficients in F. That definition by wholly undefined elements is well adapted to the treatment of difference algebras (§ 25) which are abstract algebras whose elements are certain classes of things. The same definition without postulate V is convenient in the study of algebras of infinite order (not treated in this book), an example being the field of all real numbers regarded as an algebra over the field of rational numbers.

* To emphasize this point, we may understand postulate V (that a finite basis exists) to mean that there is an upper limit to the number of linearly independent elements which can be chosen in the algebra.

CHAPTER II

LINEAR SETS OF ELEMENTS OF AN ALGEBRA

In the later investigation of an algebra A, we shall often find it necessary to consider a "linear set" of its elements which is closed under both addition and scalar multiplication. Hence we shall develop here the calculus of linear sets, including their addition and multiplication.

15. Basis, order, and intersection of linear sets. If $x_1, \ldots, x_m$ are any elements of an algebra A (not necessarily associative) over a field F, the totality of their linear combinations $\Sigma\lambda_i x_i$, whose coefficients λ_i are numbers of F, is called the *linear set** with the *basis* $x_1, \ldots, x_m$ and is designated by $(x_1, \ldots, x_m)$.

The linear set with the basis 0 is composed only of the element 0 and is called the *zero set* and is designated by (0) or 0.

The *order* of a linear set $\neq 0$ is the maximum number of linearly independent† elements which can be chosen in the set. The zero set is said to be of order zero. Hence if $x_1, \ldots, x_m$ are linearly independent, the linear set $(x_1, \ldots, x_m)$ is of order m. The set (x) is of order 1 or 0, according as $x \neq 0$ or $x = 0$.

For example, let A be the algebra of all real quaternions (§ 11). The quaternions $\alpha + \beta i$, in which α and β range over all real numbers, form the linear set $S = (1, i)$

* Called *complex* by Wedderburn and *system* by Scorza.

† With respect to the field F, as will be understood throughout. Compare § 5.

of order 2. The quaternions $ai+\beta j$ form another linear set $T=(i, j)$ of order 2.

LEMMA 1. *If $x_1, \ldots, x_n$ are n linearly independent elements of a linear set S of order $m (o<n<m)$, we can find elements $x_{n+1}, \ldots, x_m$ of S such that $S=(x_1, \ldots, x_m)$, where $x_1, \ldots, x_m$ are linearly independent.*

For, S contains elements e linearly independent of $x_1, \ldots, x_n$; select any e as x_{n+1}. Unless $m=n+1$, S contains elements f linearly independent of $x_1, \ldots, x_{n+1}$; select any f as x_{n+2}; etc.

If a linear set T contains all of the elements of a linear set S, we shall write $T \geqq S$, $S \leqq T$. If T contains S and also elements not in S, we shall write $T>S$, $S<T$.

If S and T are two linear sets of an algebra A, all elements (including certainly o) which are common to S and T evidently form a linear set. The latter is called the *intersection* of S and T, and is denoted by either $S \wedge T$ or $T \wedge S$.

In the preceding example, $S=(1, i)$, $T=(i, j)$, whence $S \wedge T=(i)$.

16. Sum. The unique linear set of smallest order which contains all the elements of S and all those of T is called the *sum* of S and T, and is denoted by either $S+T$ or $T+S$. If

(1) $S=(s_1, \ldots, s_m)$, $\quad T=(t_1, \ldots, t_n)$, then

$$S+T=(s_1, \ldots, s_m, \quad t_1, \ldots, t_n).$$

Hence $S+T$ is composed of all of the elements $\Sigma\sigma_i s_i+\Sigma\tau_j t_j$, where the σ_i and τ_j are numbers of the field F.

Since $\Sigma\sigma_i s_i$ gives all the numbers of S, and $\Sigma\tau_j t_j$ all of T, it follows that $S+T$ is the totality of those elements of A each of which is the sum of an element of S and an element of T.

If $T \leqq S$, then $S+T=S$ and conversely.

For the linear sets $S=(1, i)$ and $T=(i, j)$ of quaternions, $S+T=(1, i, j)$.

THEOREM 1. *Each element of $S+T$ is expressible in a single way as a sum of an element of S and an element of T if and only if the intersection of S and T is zero.*

For, if $s+t=s'+t'$, where s and s' are elements of S, and t and t' are elements of T, then $s-s'=t'-t$ is in the intersection $S \wedge T$ of S and T.

We readily verify that

$$(2) \quad (S+T)+U=S+(T+U), \quad (S \wedge T) \wedge U=S \wedge (T \wedge U).$$

THEOREM 2. *If two linear sets S and T are of orders m and n, while their intersection $C=S \wedge T$ is of order l, then the order of $S+T$ is $m+n-l$.*

Let $c_1, \ldots, c_l$ be linearly independent elements* of C. By Lemma 1, we may write

$$S=(c_1, \ldots, c_l, s_{l+1}, \ldots, s_m),$$
$$T=(c_1, \ldots, c_l, t_{l+1}, \ldots, t_n),$$

in which the indicated elements of S are linearly independent, and likewise those of T. Hence

$$S+T=(c_1, \ldots, c_l, s_{l+1}, \ldots, s_m, t_{l+1}, \ldots, t_n).$$

The indicated elements of $S+T$ are linearly independent. For, if

* If $C=0$, the proof holds if we suppress $c_1, \ldots, c_l$.

$$\sum_{i=1}^{l}\gamma_i c_i+\sum_{j=l+1}^{m}\sigma_j s_j+\sum_{k=l+1}^{n}\tau_k t_k=0 \qquad (\gamma_i,\ \sigma_j,\ \tau_k \text{ in } F),$$

the element $-\Sigma\tau_k t_k$ of T would be equal to the element $\Sigma\gamma_i c_i+\Sigma\sigma_j s_j$ of S and hence would be an element $\Sigma\delta_i c_i$ of their intersection C. But, by the assumption on T, the t_k and c_i are linearly independent, whence each $\tau_k=0$ and each $\delta_i=0$. Then the displayed equation becomes $\Sigma\gamma_i c_i+\Sigma\sigma_j s_j=0$, so that, by the hypothesis on S, each $\gamma_i=0$ and each $\sigma_j=0$.

The result proved for $S+T$ shows that its order is $m+n-l$.

17. Linear sets supplementary in their sum. If, for $r>2$, $S_1, \ldots, S_r$ are linear sets of an algebra A, we define the *sum* $S_1+\ldots+S_r$ by induction on r by means of

$$(3) \qquad S_1+\ldots+S_r=(S_1+\ldots+S_{r-1})+S_r.$$

Let m_i denote the order of S_i, and m the order of $S_1+\ldots+S_r$. By the preceding theorem, $m\leqq m_1+\ldots+m_r$, and the equality sign holds if and only if zero is the only element in common with $S_1+\ldots+S_{j-1}$ and S_j for $j=2, \ldots, r$, and hence, by Theorem 1, if and only if each element of $S_1+\ldots+S_r$ can be expressed in a single way in the form $s_1+\ldots+s_r$, where s_i is an element of S_i. In this case $m=m_1+\ldots+m_r$, the linear sets $S_1, \ldots, S_r$ are said to be *supplementary* in $S_1+\ldots+S_r$.

In particular, S_1 and S_2 are supplementary in S_1+S_2 if and only if $S_1\frown S_2=0$. For example, (i, j) and $(1, k)$ are supplementary in their sum $(1, i, j, k)$.

LEMMA 2. *If S and T are linear sets of an algebra A and if $T \leqq S$, we can find a linear set X such that T and X are supplementary, i.e., $S = T + X$, $T \wedge X = 0$.*

This follows from Lemma 1 by taking

$$T = (x_1, \ldots, x_n), \qquad X = (x_{n+1}, \ldots, x_m).$$

However, if $T < S$, X is not uniquely determined by S and T since we may replace the foregoing special X by

$$(x'_{n+1} + t_{n+1}, \ldots, x'_m + t_m),$$

where the t's are any elements of T, while $x'_{n+1}, \ldots, x'_m$ are any $m-n$ linearly independent elements of X.

18. Product of linear sets. If S and T are any linear sets of an algebra A, the linear set of minimum order, which contains all elements obtained by multiplying each element of S by each element of T, is called the *product* of S by T, and is denoted by ST. Hence, in the notation (1),

$$(4) \quad (s_1, \ldots, s_m)(t_1, \ldots, t_n) = (s_1 t_1, \ldots, s_1 t_n, s_2 t_1, \ldots, s_m t_n),$$

and the order of ST is $\leqq mn$. From (1),

$$(5) \quad (S+T)U = SU + TU, \qquad U(S+T) = US + UT.$$

Usually $ST \neq TS$. When A is an associative algebra, $(ST)U = S(TU)$.

Consider the special case in which $S = (s)$ is composed of the scalar products of s by the various numbers of the field F. Then

$$ST = (s)(t_1, \ldots, t_n) = (st_1, \ldots, st_n)$$

coincides with the products of s by the various elements $\Sigma\tau_i t_i$ of T. Hence we shall often write sT in place of $(s)T$. By (5),

$$P \equiv [(x)+(y)]U = (x)U+(y)U = xU+yU.$$

Since the elements of $(x+y)U$ occur in P,

$$(x+y)U \leqq xU+yU. \tag{6}$$

This becomes $0 \leqq xU$ when $y=-x$, whence $yU=xU$. Hence in (6) the sign may be $<$ and not $=$.

LEMMA 3. *If the order of sT (or Ts) is less than that of T, there exists an element $x \neq 0$ of T such that $sx=0$ (or $xs=0$), and conversely.*

For, we may write $T=(t_1, \ldots, t_n)$, where $t_1, \ldots, t_n$ are linearly independent with respect to F. If $sx \neq 0$ for every $x=\Sigma\tau_i t_i$ in which $\tau_1, \ldots, \tau_n$ are numbers not all zero of F, then $st_1, \ldots, st_n$ are linearly independent, and sT is of the same order n as T.

Conversely, if $sx=0$ for at least one such x, then $st_1, \ldots, st_n$ are linearly dependent, and sT is of order $<n$.

Denote the intersection $A \wedge B$ of two linear sets A and B by T, and consider the product ST given by (4). Since each element t_j of T is in both A and B, each product $s_i t_j$ is in both SA and SB and hence is in their intersection. Hence

$$S(A \wedge B) \leqq SA \wedge SB. \tag{7}$$

For example, let $A=(1, i, j, k)$ be the algebra of real quaternions, and $S=(1, i)$, $T=(i, j)$. Then

$$S^2=S,\ ST=TS=A,\quad S \wedge T=(i),\quad T^2=(1, k)=T(S \wedge T) = TS \wedge T^2.$$

CHAPTER III*

INVARIANT SUB-ALGEBRAS, DIRECT SUM, REDUCIBILITY, DIFFERENCE ALGEBRAS

In the later development of the theory of algebras, we shall need certain tools and concepts which are analogous to processes and ideas employed in the theory of groups and were in fact borrowed from that theory. However, we shall explain them fully without reference to groups.

19. Sub-algebra. A linear set S of elements of an algebra A over a field F is called a *sub-algebra* of A if $S \neq 0$, $S^2 \leqq S$. If also $S < A$, S is called a *proper* sub-algebra of A. Note that $S^2 \leqq S$ implies that S is closed under multiplication.

For example. the totality of elements of A which are commutative with a given element $e \neq 0$ of A is a sub-algebra if A is associative. If A contains elements which are commutative with *every* element of A, all such elements form a sub-algebra, called the *central* of A. The only quaternions commutative with i are $\alpha + \beta i$, which form a proper sub-algebra S. Those commutative with k are $\alpha + \beta k$. Hence the central is composed of the scalar multiples α of the unit 1.

20. Invariant sub-algebra. If B is a linear set of elements of an algebra A such that $B \neq 0$, $AB \leqq B$, $BA \leqq B$, then B is an algebra which is called an *invariant* sub-algebra of A. That B is an algebra follows from $B \leqq A$, $B^2 \leqq BA \leqq B$.

* The associative law of multiplication is not assumed in chap. iii.

An invariant proper sub-algebra B of A is called *maximal* if there does not exist in A an invariant proper sub-algebra which contains B and is distinct from B.

For example, $B=(u_1)$ is an invariant proper sub-algebra of

$$(1)\quad A=(u_1, u_2, u_3): \qquad u_i^2=u_i, \qquad u_iu_j=u_ju_i=0 \ (j\neq i).$$

But B is not maximal since it is contained in the (maximal) invariant proper sub-algebra (u_1, u_2) of A.

THEOREM 1. *If B_1 and B_2 are invariant sub-algebras of an algebra A, then B_1+B_2 is an invariant sub-algebra of A.*

For,

$$A(B_1+B_2)=AB_1+AB_2\leqq B_1+B_2, \qquad (B_1+B_2)A\leqq B_1+B_2.$$

If also B_1 is maximal, then either $B_1+B_2=A$ or else B_1+B_2 is an invariant proper sub-algebra (of A) which contains B_1 and hence coincides with B_1, so that $B_2\leqq B_1$.

COROLLARY. *If B_1 and B_2 are distinct maximal invariant sub-algebras of A, then $B_1+B_2=A$.*

THEOREM 2. *If B_1 and B_2 are invariant sub-algebras of A, their intersection C is either zero or an invariant sub-algebra of A.*

For, $CA\leqq B_1A\leqq B_1$ and $CA\leqq B_2A\leqq B_2$ imply $CA\leqq C$. Similarly, $AC\leqq C$.

21. Direct sum, reducible algebras. If an algebra A is expressible as the sum of two proper sub-algebras B and C, such that

$$BC=0, \qquad CB=0, \qquad B\wedge C=0,$$

then A is said to be the *direct sum* of B and C, and to be *reducible* into the *components* B and C. We shall then write $A = B \oplus C = C \oplus B$.

Let A have the modulus u. Then $u = e + f$, where e is in B, and f is in C. Then e is the modulus of B. For, if b is any element of B, then $bf = 0 = fb$, whence $b = bu = be$, $b = ub = eb$. Similarly, f is the modulus of C.

For example, algebra (1) with the modulus $u_1 + u_2 + u_3$ is the direct sum of (u_1) and (u_2, u_3) with the moduli u_1 and $u_2 + u_3$. It is also reducible into the components (u_2) and (u_1, u_3). Moreover, $A = (u_3) \oplus (u_1, u_2)$.

LEMMA. *If B and C are sub-algebras, either of which has a modulus,* and if $BC = 0 = CB$, then $B \wedge C = 0$, so that the sum of B and C is their direct sum.*

For, if B has the modulus e, denote by I the intersection $B \wedge C$ of B and C. Since e is a modulus and $I \leqq B$, $eI = I$, while $eI = 0$ since e is in B and $I \leqq C$. Hence $I = 0$.

22. Theorem. *If any algebra A has an invariant proper sub-algebra B which possesses a modulus b satisfying the associative relations*

$$(2) \quad b \cdot xy = bx \cdot y, \qquad x \cdot yb = xy \cdot b, \qquad x \cdot by = xb \cdot y,$$

for all elements x and y of A, then A is reducible and has B as one component.

For, by Lemma 2 of § 17, we can find a linear set C' such that $A = B + C'$, $B \wedge C' = 0$. Let $y_1', \ldots, y_r'$ form a basis of C' and write

$$y_i = y_i' - by_i' - y_i'b + by_i'b \qquad (i = 1, \ldots, r).$$

* If neither B nor C has a modulus, we may have $BC = 0 = CB$, $B \wedge C \neq 0$, as in the case $B = (u_1, u_2)$, $C = (u_1, u_3)$, where $u_1^2 = 0$, $u_2^2 = u_3^2 = u_1$, $u_i u_j = 0 (i \neq j)$.

We shall prove that A reduces into the component algebras B and C, where C is the linear set $(y_1, \ldots, y_r)$. Since b is in the invariant sub-algebra B of A, by_i', etc., belong to B. Hence if a_i is any number of the field over which A is defined, $\Sigma a_i y_i = \Sigma a_i y_i' + b'$, where b' belongs to B. Thus

$$B+C=B+C'=A.$$

If x is any element of B,

$$xy_i = xy_i' - xb \cdot y_i' - xy_i'b + xb \cdot y_i'b = 0,$$

since $xb=x$. Similarly, $y_ix=0$. Hence $BC=0$, $CB=0$. The theorem will therefore follow from the preceding lemma if we prove that C is an algebra. For that proof consider any element $z=x+y$ of A, where x is in B and y is in C. Since

$$yb=0=by, \qquad xb=x=bx,$$

we find that

$$Z \equiv z - bz - zb + bzb$$

cancels to y and hence is in C. If we replace z by yc, where c is any element of C, we find that Z reduces to its first term yc. This proves that the product of any two elements y and c of C is in C, which is therefore an algebra.

23. Lemma. *If $A=B\oplus C$ and if B has a modulus b, then b is commutative with every element of A and the associative relations* (2) *hold.*

Let $x=u+v$, and $y=w+z$ be any elements of A, where u and w are in B, and v and z are in C. Then

$$bx=bu+bv=bu=u, \qquad xb=ub+vb=ub=u,$$

so that b is commutative with every x. Next,

$$b \cdot xy = b \cdot (u+v)(w+z) = b(uw+vz) = uw,$$
$$bx \cdot y = uy = u(w+z) = uw,$$

which proves the first relation (2). The remaining two are proved similarly.

24. Theorem. *Any reducible algebra A with a modulus* m can be expressed as a direct sum of irreducible algebras, each with a modulus, in one way and only one way apart from the arrangement of the component algebras*

Since A is reducible, $A = B \oplus C$. Then m is the sum of the moduli of B and C (§ 21). If either B or C is reducible we replace it by the direct sum of two components. This process terminates since A is of finite order. Hence A is a direct sum of irreducible algebras $A_1, \ldots, A_m$ each with a modulus.

If possible, let A be also the direct sum of the irreducible algebras $B_1, \ldots, B_n$. Let a_i be the modulus of A_i, and b_i that of B_i. Then $m = \Sigma a_i = \Sigma b_i$ is the modulus of A. Let j be any chosen one of $1, \ldots, n$. Since $B_j = mB_j = \Sigma a_i B_j$, there is a value of i for which $P = a_i B_j$ is not zero. Since A_i is invariant in A, $P \leqq A_i$. If x is in B_j, we see by § 23 with $B = A_i$ that

$$a_i x \cdot a_i b_j = a_i^2 x b_j = a_i x b_j = a_i x,$$

whence P has the modulus $a_i b_j$. Since B_j is invariant in A,

$$A_i P = a_i A_i B_j \leqq a_i B_j = P, \quad P A_i \leqq P.$$

* If A has no modulus, it may be expressible in more than one way as a direct sum of irreducible algebras. For example, if $A = (u, v)$, where $u^2 = uv = vu = v^2 = 0$, then $A = (x) \oplus (y)$, where x and y are any two linearly independent elements of A.

Hence A_i has the invariant sub-algebra P which has a modulus. If it were a proper sub-algebra, A_i would be reducible* (§ 22), contrary to hypothesis. Hence $P=A_i$. But P is invariant also in B_j, which is irreducible. As before, $P=B_j$. Hence each algebra B_j is identical with one of the $A_1, \ldots, A_m$.

For further theorems on reducible algebras, see Appendix III.

25. Difference algebra. This abstract concept is analogous to that of quotient-groups in the theory of finite groups. To provide a preliminary illustration, consider the (associative) algebra A over a field F with the multiplication table

	u_1	u_2	u_3	u_4
u_1	u_1	u_2	u_3	u_4
u_2	u_2	0	0	u_2
u_3	u_3	0	0	u_3
u_4	u_4	$-u_2$	u_3	u_1

The product u_iu_j is found in the body of the table at the intersection of the line through the left-hand label u_i and the column having the label u_j at its top. For example, $u_2u_4=u_2$, $u_4u_2=-u_2$. It has the invariant sub-algebra $B=(u_2, u_3)$.

To each number $x=\xi_1u_1+\ldots+\xi_4u_4$ of A we make correspond the number $x'=\xi_1v_1+\xi_4v_4$ of the (associative) algebra

$$D=(v_1, v_4): \quad v_1^2=v_1, \quad v_1v_4=v_4, \quad v_4v_1=v_4, \quad v_4^2=v_1,$$

* By § 23 with $B=B_j$, $b_j \cdot xy=b_jx \cdot y$. Let x and y be any elements of A_i, whose modulus is a_i. Hence the foregoing formula gives $b_j \cdot a_i(xy) = b_j(a_ix) \cdot y$ and hence also $b_ja_i \cdot xy=(b_ja_i)x \cdot y$. But $b_ja_i=a_ib_j$ is the modulus of P. This proves the first formula (2) for algebra A_i. The other two follow similarly.

over the same field F. To the sum of any two numbers x and $y=\eta_1 u_1+\ \ldots\ .+\eta_4 u_4$ of A evidently corresponds the sum of their corresponding numbers x' and $y'=\eta_1 v_1+\eta_4 v_4$ of D. To ρx, where ρ is in F, corresponds $\rho x'$. To

$$xy=(\xi_1\eta_1+\xi_4\eta_4)u_1+(\xi_1\eta_2+\xi_2\eta_1+\xi_2\eta_4-\xi_4\eta_2)u_2 \\ +(\xi_1\eta_3+\xi_3\eta_1+\xi_3\eta_4+\xi_4\eta_3)u_3+(\xi_1\eta_4+\xi_4\eta_1)u_4$$

corresponds

$$(\xi_1\eta_1+\xi_4\eta_4)v_1+(\xi_1\eta_4+\xi_4\eta_1)v_4=x'y'.$$

Hence our correspondence (which amounts to suppressing all scalar multiples of the units u_2 and u_3 of B) is preserved under addition, scalar multiplication, and multiplication.

The algebra D so determined by A and B is called their *difference algebra* and is designated by $A-B$.

Next, let us employ, in place of B, the algebra $S=(u_1,\ u_2)$, over F, which is not invariant in A since $u_3u_1=u_3$ is not in S. To x we now make correspond the number $x_0=\xi_3 w_3+\xi_4 w_4$ of the algebra

$$D_0=(w_3\,,\ w_4):\qquad w_3^2=0,\qquad w_3w_4=w_3,\qquad w_4w_3=w_3,\qquad w_4^2=0,$$

so that in effect we suppress all scalar multiples of the units u_1 and u_2 of S. To xy now corresponds

$$(\xi_1\eta_3+\xi_3\eta_1+\xi_3\eta_4+\xi_4\eta_3)w_3+(\xi_1\eta_4+\xi_4\eta_1)w_4\,,$$

which is not equal to $x_0y_0=(\xi_3\eta_4+\xi_4\eta_3)w_3$, so that the correspondence is not preserved under multiplication. Nor is D_0 an associative algebra since

$$w_3w_4^2=0\,,\qquad w_3w_4\cdot w_4=w_3w_4=w_3\,.$$

To treat the general case, let B be a linear set of elements of an algebra A over a field F. Two elements x and y of A are called *congruent* or *incongruent* with respect to B as modulus (or briefly, modulo B), according as $x-y$ is or is not an element of B. In the respective cases, we write

$$x \equiv y \pmod{B}, \qquad x \not\equiv y \pmod{B}.$$

If $x \equiv y$ and $x \equiv z \pmod{B}$, then

$$y-x=-(x-y), \qquad y-z=(x-z)-(x-y)$$

are elements of B, so that $y \equiv x$, $y \equiv z \pmod{B}$. The first shows that the members of a congruence may be interchanged. The second shows that all those elements of A which are congruent to a given element x modulo B are congruent to each other; they are said to form a *class* $[x]$ modulo B. Hence all elements of A may be distributed into non-overlapping classes modulo B.

If a is any number of F, and if $x \equiv y$, $x' \equiv y' \pmod{B}$, then

$$ax=xa \equiv ay=ya, \qquad x+x' \equiv y+y' \pmod{B}.$$

Hence the product, in either order, of a and any element y of the class $[x]$ is in the class $[ax]=[xa]$, while the sum of any element y of class $[x]$ and any element y' of class $[x']$ is in the class $[x+x']$. Accordingly, we define the scalar product $a[x]=[x]a$ of the number a of F and the class $[x]$ to be the class $[ax]$, and define the sum of the classes $[x]$ and $[x']$ to be the class $[x+x']$. Hence the linear function $\Sigma a_i[x_i]$ of the classes $[x_i]$ with coefficients a_i in F is the class $[\Sigma a_i x_i]$.

Let T be a linear set supplementary to B in A, so that $T \wedge B = 0$ and every element a of A is expressible

in one and only one way as a sum of an element b of B and an element t of T (§§ 16, 17). If also $a_1 = b_1 + t_1$ and if $a \equiv a_1 \pmod{B}$, then $t \equiv t_1 \pmod{B}$, and $t - t_1$ is common to B and T and hence is zero. Hence if $a = b + t$ and $a_1 = b_1 + t_1$ are in the same class, $t = t_1$. Thus there is a (1, 1) correspondence between the classes of A modulo B and the elements of T.

If $a_i = b_i + t_i$, where b_i is in B and t_i is in T, the class $\Sigma a_i[a_i]$ corresponds to $\Sigma a_i t_i$ in T. The number of linearly independent t_i is $n - m$ if B is of order m and A is of order n. Hence we may select $n - m$ classes of A modulo B such that every class of A modulo B is expressible in one and only one way as a linear function of those $n - m$ classes with coefficients in F.

We now assume that B is an invariant sub-algebra of A. Again let $x \equiv y$, $x' \equiv y' \pmod{B}$, whence $y = x + b$, $y' = x' + b'$, where b and b' are elements of B. Then

$$yy' = xx' + xb' + by' \equiv xx' \pmod{B},$$

since xb' and by' are elements of the invariant sub-algebra B of A, whence their sum is in B. Hence the product of any element y of class $[x]$ by any element y' of class $[x']$ is an element of the class $[xx']$. Accordingly, we define the product $[x]\,[x']$ of the class $[x]$ by the class $[x']$ to be the class $[xx']$.

THEOREM 1. *If B is an invariant proper sub-algebra of order m of an algebra A of order n over a field F, the classes of A modulo B are the elements of an algebra of order $n - m$ over F when addition, scalar multiplication, and multiplication of classes $[x]$ are defined by*

$$[x] + [x'] = [x + x'], \quad a[x] = [x]a = [ax], \quad [x][x'] = [xx'], \quad a \text{ in } F.$$

For, postulates I–IV of § 4 are seen to hold, and, as shown above, $n-m$ classes serve as a finite basis.

The resulting algebra of classes is called the *difference algebra* $A-B$, and also the *algebra complementary to* B *in* A. Evidently $A-B$ is an associative algebra when A is one.

Let T be any linear set supplementary to B in A. We saw above that the elements of T are in (1, 1) correspondence with the classes of A modulo B, and this correspondence is preserved under addition and scalar multiplication, but not in general under multiplication since T need not be closed under multiplication. However, we may regard the elements of T as the elements of an algebra T' in which addition and scalar multiplication are defined as in T, while the product in T' of any two elements x and y of T' (i.e., the same elements of T) is defined to be the element of T which belongs to the class modulo B containing the product in A of x and y. This algebra T' is therefore equivalent to $A-B$ and is said to be obtained by taking T modulo B. Since $A=B+T$, this amounts to taking A modulo B.

In our introductory example, $A=(u_1, u_2, u_3, u_4)$, $B=(u_2, u_3)$. Then $T=(u_1, u_4)$ is supplementary to B in A. By chance, T is itself an algebra and plays the rôle of T'. Thus $A-B$ is equivalent to T, as is implied in the discussion of the example. As a generalization of this example, we have the following

THEOREM 2. *If A is the direct sum of algebras B and T, then T is equivalent to $A-B$, and B is equivalent to $A-T$.*

For, $BA=B(B+T)=B^2\leqq B$, $AB=B^2\leqq B$, so that B (and similarly T) is an invariant sub-algebra of A. Moreover, the product (in A) of any two elements x and

y of T is in the sub-algebra T, which therefore plays the rôle of T' above.

A better illustration of T' is furnished by the associative algebra

$$A=(u_1, u_2, u_3): \quad u_1u_i=u_iu_1=u_i \quad (i=1, 2, 3),$$
$$u_2u_3=u_3u_2=u_3^2=0, \quad u_2^2=u_3.$$

Then $B=(u_3)$ is evidently invariant in A. The simplest T is (u_1, u_2), which is not an algebra since $u_2^2=u_3$. Then $T'=(v_1, v_2)$, where

$$v_1v_j=v_jv_1=v_j \quad (j=1, 2), \quad v_2^2=0,$$

the final equation replacing $u_2^2=u_3$ when we take T modulo $B=(u_3)$.

26. Theorem. *If B_1 and B_2 are invariant proper sub-algebras of A and if $B_2<B_1$, then $A-B_2$ contains an invariant proper sub-algebra which is equivalent to B_1-B_2.*

For, B_2 is evidently invariant in B_1. Elements of B_1 congruent modulo B_2 are elements of A congruent modulo B_2, whence each class of B_1 modulo B_2 is contained in a unique class of A modulo B_2. Hence those classes of A modulo B_2 which contain the various classes of B_1 modulo B_2 constitute (in $A-B_2$) a proper sub-algebra S equivalent to B_1-B_2.

To prove that S is invariant in $A-B_2$, let x and y be any elements of A and B_1, respectively. Then xy and yx are elements of B_1 since it is invariant in A. Passing to the corresponding classes $[x]$ and $[y]$ of A modulo B_2, we see that $[x]$ is an element of $A-B_2$, and that $[y]$, $[x]$ $[y]$, and $[y]$ $[x]$ are elements of S, whence S is invariant in $A-B_2$.

27. We next prove the converse of the last theorem:

THEOREM. *If B_2 and S are invariant proper sub-algebras of A and $A-B_2$, respectively, then A has an invariant proper sub-algebra B_1 such that $B_2<B_1$ and B_1-B_2 is equivalent to S.*

For, all those elements x of A which belong to classes $[x]$, of A modulo B_2, giving elements of S constitute a sub-algebra B_1 of A. Since S is a proper sub-algebra of $A-B_2$, $B_1<A$. Since $[0]=B_2$, we have $B_2<B_1$. If $[x]$ is an element of S, and $[y]$ is an element of $A-B_2$, the invariance of S in $A-B_2$ shows that $[xy]$ and $[yx]$ are elements of S. Hence if x is in B_1, and y is in A, then xy and yx are in B_1, which is therefore invariant in A.

28. Simple algebras. An algebra having no invariant proper sub-algebra is called *simple*. Every algebra of order 1 is simple since it has no proper sub-algebra.

The theorem of § 26 evidently implies

COROLLARY 1. *If B_2 is an invariant proper sub-algebra of A and if $A-B_2$ is simple, then B_2 is a maximal invariant proper sub-algebra of A.*

We readily prove the converse:

COROLLARY 2. *If B_2 is a maximal invariant proper sub-algebra of A, then $A-B_2$ is simple.*

For, if $A-B_2$ were not simple, it would have an invariant proper sub-algebra S and, by the theorem of § 27, A would have an invariant proper sub-algebra $B_1>B_2$, whereas B_2 is maximal.

CHAPTER IV

NILPOTENT AND SEMI-SIMPLE ALGEBRAS; IDEMPOTENT ELEMENTS

We shall develop here the properties of important special types of algebras which play leading rôles in the theory of general algebras. That theory depends also upon a knowledge of the properties of various kinds of idempotent elements each of which is equal to its own square.

29. Index. If A is any associative* algebra, $A^2 \leqq A$, whence $A \cdot A^2 \leqq A \cdot A$, or $A^3 \leqq A^2$, and similarly $A^{k+1} \leqq A^k$ for every positive integer k. If the inequality sign held for every k, the orders of A, A^2, A^3, ... would form an infinite series of decreasing positive integers. Hence there exists a least positive integer a such that $A^{a+1} = A^a$, and therefore

$$A > A^2 > A^3 > \ldots . > A^{a-1} > A^a, \qquad A^t = A^a (t > a).$$

This a is called the *index* of A.

For example, consider the associative algebra,

$$A = (u_1, u_2): \qquad u_1^2 = u_1 u_2 = u_2 u_1 = u_2^2 = \beta u_1$$

over a field F containing β. If $\beta \neq 0$, $A^2 = (u_1) = A^3$; if $\beta = 0$, $A^2 = 0 = A^3$. In either case, $A > A^2$, and A is of index 2.

30. Nilpotent algebras. If $A^a = 0$, A is called *nilpotent.* In particular, if $A^2 = 0$, A is called a *zero algebra;* the product of any two of its elements is zero.

* Henceforth in the book, multiplication is assumed to be associative, unless the contrary is expressly stated.

The algebra in the preceding example is nilpotent if and only if $\beta=0$. The algebra

$$B=(v_1, v_2): \qquad v_1^2=v_2,\ v_1v_2=v_2v_1=v_2^2=0$$

is nilpotent and of index 3.

THEOREM. *If an algebra A has a maximal nilpotent invariant sub-algebra N, every nilpotent invariant sub-algebra N_1 of A is contained in N.*

For, by Theorem 1 of § 20, $N+N_1$ is an invariant sub-algebra of A. To prove that it is nilpotent, let N_2 denote the intersection of N and N_1, and let P be any product formed of two or more factors N and N_1, but not a power of either. Since N is invariant in A and occurs as a factor of P, we have $P\leqq N$. Similarly, $P\leqq N_1$. Hence $P\leqq N_2$. Thus

$$(N+N_1)^\alpha\leqq N^\alpha+N_1^\alpha+N_2, \qquad \alpha\geqq 2.$$

If α is the greater of the indices of the nilpotent algebras N and N_1, we have

$$N^\alpha=N_1^\alpha=0, \qquad (N+N_1)^\alpha\leqq N_2, \qquad (N+N_1)^{\alpha^2}\leqq N_2^\alpha\leqq N^\alpha=0,$$

so that $N+N_1$ is nilpotent. It was seen to be invariant in A. But N is a maximal nilpotent invariant sub-algebra of A. Hence $N_1\leqq N$.

31. Idempotent elements. An element $e\neq 0$ such that $e^2=e$ is called idempotent. Since every power of e reduces to e, e is not nilpotent. In an algebra having a modulus m, m is idempotent.

THEOREM. *Every algebra P which is not nilpotent contains an idempotent element.*

Let α denote the index of P, so that $A\equiv P^\alpha\neq 0$, $P^{\alpha+1}=P^\alpha$. Thus $A^2=A$. Since every number of algebra

A is in P, the theorem will follow if we prove that A contains an idempotent element. We shall establish this by induction, assuming that every non-nilpotent algebra whose order is less than the order of A contains an idempotent element. Note that the theorem holds when P is of order 1 since P is then composed of the scalar products of an element u such that $u^2=\beta u$, $\beta\neq 0$, whence u/β is idempotent.

First, let A contain an element a such that $Aa=A$. Then every element y of A is in Aa and is therefore expressible as a product za of an element z of A by a and, in fact, in a single way. For, if also $y=z'a$, then $(z-z')a=0$, whence $z-z'=0$ by the converse of the lemma in § 18 with $s=a$, $x=z-z'$, $T=A$.

In particular, the element a of A is expressible in a single way in the form wa, where w is in A and $w\neq 0$. Since $wa=w\cdot wa$, $a=w^2a$ and hence $w^2=w$. Hence A contains the idempotent element w.

Second, let A contain no element a such that $Aa=A$, whence $Ax<A$ for every x in A. For a fixed x, Ax is an algebra since

$$Ax\cdot Ax=AxA\cdot x\leqq Ax.$$

If Ax is not nilpotent, it contains an idempotent element e by the assumption for the induction, and e belongs to A.

Finally, let Ax be nilpotent for every x in A. Hence $(Ax)^l=0$ for l sufficiently large. From $A^2=A$, we see by induction on k that

$$(AxA)^k=(Ax)^kA,$$

which is zero if $k=l$. Hence AxA is nilpotent and is an algebra since its square is $AxA\cdot xA\leqq AxA$, and is evi-

dently invariant in A. Hence by the theorem in § 30, $AxA \leqq N$, where N is the maximal nilpotent invariant sub-algebra of A. When x ranges over all elements of A, the totality of elements in the algebras AxA constitutes $A^3 = A$. Hence $A \leqq N$, whereas A is not nilpotent. Since our final case is excluded, the theorem is proved.

COROLLARY. *An algebra is nilpotent if all its elements are nilpotent.*

32. Properly nilpotent elements. Let A be an algebra with a (unique, § 30) maximal nilpotent invariant sub-algebra N. If a is in N, ax and xa are in N and hence are nilpotent for every x in A, since N is invariant.

We shall call an element $a \neq 0$ of A *properly nilpotent* in A if ax and xa are nilpotent for every x in A. Taking $x = a$, we see that a^2 and hence a itself is nilpotent. As noted above, all elements $\neq 0$ of N are properly nilpotent in A.

But not every nilpotent element is properly nilpotent. For, if

$$a = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad x = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \qquad p = \begin{pmatrix} 0 & 0 \\ \alpha & \beta \end{pmatrix},$$

then $a^2 = 0$ and a is nilpotent. But $ax = p$, and, for $\beta = 1$, $p^2 = p \neq 0$, so that p is idempotent. Hence ax is not nilpotent for every x. Thus a is nilpotent, but not properly nilpotent, in the algebra* of all two-rowed matrices.

If ax is nilpotent, there exists a positive integer r such that

$$(ax)^r = 0, \qquad (xa)^{r+1} = x(ax)^r a = 0,$$

* It is simple (§ 52) and hence, by the theorem of this section, has no properly nilpotent element. By means of the quadratic equation (§ 59) $\omega^2 - (\alpha+\delta)\omega + \alpha\delta - \beta\gamma = 0$ satisfied by x, it follows that x is nilpotent if and only if its determinant is zero and $\alpha + \delta = 0$.

whence also xa is nilpotent, and conversely. Hence an element $a \neq o$ is properly nilpotent in A if either ax or xa is nilpotent for every x in A.

THEOREM. *An algebra A contains properly nilpotent elements if and only if it possesses a maximal nilpotent invariant sub-algebra N, and then the properly nilpotent elements of A coincide with the elements $\neq o$ of N.*

The proof falls into four steps.

i) If a is properly nilpotent in A, and if b is any element of A, then each of ba and ab is o or properly nilpotent in A.

For, if x is any element of A, $x \cdot ba = (xb)a$ and $ab \cdot x = a(bx)$ are nilpotent by the definition of a. Hence ba and ab are o or properly nilpotent.

ii) If a is properly nilpotent in A, and if b and c are any elements of A, then bac belongs to N.

For, suppose that bac is not zero and hence is properly nilpotent by (i). Then AaA is not zero and is evidently an invariant sub-algebra of A. Since AaA is also nilpotent, it is contained in N by the theorem of § 30.

iii) If a and b are properly nilpotent in A, then $a+b$ is o or properly nilpotent.

For, let $a+b \neq o$. Since

$$(a+b)^3 = a^3+aba+ba^2+b^2a+a^2b+ab^2+bab+b^3$$

is a sum of elements belonging to N by (ii), $(a+b)^3$ is in N. Thus $a+b$ is nilpotent. Next, let z be any element of A. By (i), each of az and bz is o or properly nilpotent. Hence their sum $(a+b)z$ is o or nilpotent by the result just proved. By definition, $a+b$ is properly nilpotent.

iv) In view of (i) and (iii) and the evident fact that any scalar product of any properly nilpotent element is o

or properly nilpotent, it follows that, if an algebra A possesses properly nilpotent elements, the totality of them, together with o. constitute a sub-algebra which is nilpotent and invariant in A. It is contained in N by the theorem of § 30. It coincides with N since we noted above that all elements $\neq 0$ of N are properly nilpotent.

33. Decomposition relative to an idempotent element. Let A be an algebra containing at least one idempotent element e. Write

$$x_1 = x - ex - xe + exe, \qquad x_2 = ex - exe, \qquad x_3 = xe - exe,$$
$$I = \Sigma x_1, \qquad B = \Sigma(ex - xe),$$

where the summations extend over all elements x of A. Then

$$eB = \Sigma x_2, \qquad Be = \Sigma(-x_3) = \Sigma x_3, \qquad eAe = \Sigma exe,$$

$$eI = 0, \qquad Ie = 0, \qquad eBe = 0. \tag{1}$$

Since

$$x = x_1 + x_2 + x_3 + exe,$$

$$A = I + eB + Be + eAe, \tag{2}$$

where those of these four linear sets which are not zero are supplementary in their sum A. For, if

$$x = a + b + c + d,$$

where a, b, c, d are elements of I, eB, Be, eAe, respectively, we see from (1) that $ex = b + d$, $xe = c + d$, $exe = d$, whence $d = exe$, $c = x_3$, $b = x_2$, $a = x_1$, and are uniquely determined by x.

Hence $xe=0$ implies $c=d=0$, $x=a+b$. Thus $R=I+eB$ is composed of all those elements x of A for which $xe=0$. Similarly, $L=I+Be$ is composed of all those elements y of A for which $ey=0$. We express these results by

$$(3)\quad R=I+eB, \qquad Re=0, \qquad L=I+Be, \qquad eL=0.$$

Evidently $eR=eB$, $Le=Be$. Hence (2) implies

$$(4)\qquad A=I+eR+Le+eAe,$$

which is called *the decomposition of A relative to the idempotent element e.*

Note that I is the intersection of R and L, being composed of all those elements x of A for which both $ex=0$ and $xe=0$. We shall call I the part of A *annihilated* by e. By (2),

$$Ae=Be+eAe, \qquad eA=eB+eAe,$$

whence

$$(5)\qquad A=R+Ae, \qquad A=L+eA.$$

34. Principal idempotent elements. An idempotent element e of an algebra A is called a *principal* idempotent (for A) if there does not exist in A an idempotent u such that $eu=ue=0$. In other words, e is a principal idempotent for A if and only if the part I annihilated by e has no idempotent element and hence (§ 31) if and only if I is 0 or a nilpotent algebra.

If A has a modulus m, evidently m is a principal idempotent of A, and is the only one. For, if e were a principal idempotent $\neq m$, then $u=m-e$ is idempotent and $eu=ue=0$, whence e would not be principal.

THEOREM. *If an algebra A contains an idempotent element e, either e is a principal idempotent or A contains at least one principal idempotent element $e+u$, where u is idempotent and $eu=0=ue$.*

For, if e is not principal, we have (4), where I contains an idempotent u which (like every element of I) has the property $eu=ue=0$. Then $e'=e+u$ is idempotent since

$$e'^2=e^2+eu+ue+u^2=e+u=e', \qquad ee'=e^2=e, \qquad e'\neq 0.$$

Let I' be the part of A annihilated by e'. If I' is 0 or nilpotent, e' is the desired principal idempotent for A. In the contrary case, we repeat the discussion with e' in place of e. The process terminates since $I>I'>I''$ . . . . For, if w is any element of I', $we'=e'w=0$ by the definition of I'. Then

$$0=we'\cdot e=w(e+u)e=we, \qquad 0=e\cdot e'w=ew,$$

so that w is in I. Also, u is in I, but is not in I' since $ue'=u\neq 0$.

35. Lemma. *If e is a principal idempotent element of A, every element $\neq 0$ of I, L, and R in (4) is properly nilpotent.*

By (3), each element of LR is annihilated by e and hence belongs to I. Since e is a principal idempotent, I is 0 or nilpotent. Hence there exists a positive integer k such that

$$(LR)^k=0, \qquad (RL)^{k+1}=R(LR)^kL=0,$$

so that also RL is 0 or nilpotent.

Since R is composed of all those elements of A for which $Re=0$, we have $AR\cdot e=0$, whence $AR\leqq R$,

$A \cdot RL \leqq RL$. Similarly, $LA \leqq L$, $RL \cdot A \leqq RL$. Hence RL is o or a nilpotent invariant sub-algebra of A. By (5) and (3),

$$AL = RL + A \cdot eL = RL, \qquad RA = RL + Re \cdot A = RL.$$

Hence AL and RA, like RL, are o or nilpotent, so that each element of L and R is o or properly nilpotent. The same is true of their intersection I.

Now $AR \leqq R$ implies $eR \leqq R$. Similarly, $Le \leqq L$. This proves the

COROLLARY. *If e is a principal idempotent element, each element of the first three parts I, eR, Le of (4) is zero or properly nilpotent. If all are zero, $A = eAe$ has the modulus e.*

36. Theorem. *Every algebra without a modulus has a nilpotent invariant sub-algebra.*

Let A be an algebra which is not nilpotent. By § 31, A contains an idempotent element and hence, by § 34, contains a principal idempotent element e. By the preceding corollary, either e is a modulus for A, or A contains properly nilpotent elements and therefore (§ 32) has a nilpotent invariant sub-algebra.

37. Semi-simple algebras. An algebra having no nilpotent invariant proper sub-algebra is called *semi-simple*. Hence (§ 28) a simple algebra is semi-simple.

For example, a direct sum of two or more simple algebras A_i, no one being a zero algebra of order 1, is not simple since each A_i is invariant, but is semi-simple (§ 40).

Consider a semi-simple algebra A which is nilpotent. If the index of A exceeds 2, then $A > A^2 \neq o$, and A^2 is a nilpotent invariant proper sub-algebra of A, whereas A

is semi-simple. Hence A is a zero algebra (i.e., $A^2=0$). Then any element $a\neq 0$ of A determines a nilpotent invariant sub-algebra (a) of order 1. Since the latter is not a proper sub-algebra, it coincides with A, which is therefore of order 1.

THEOREM 1. *A semi-simple algebra is nilpotent if and only if it is a zero algebra of order* 1.

Consider a semi-simple algebra A without a modulus. By § 36, it has a nilpotent invariant sub-algebra, which is not proper and hence coincides with A. Hence the preceding theorem yields

THEOREM 2. *Any semi-simple algebra has a modulus unless it is a zero algebra of order* 1.

38. Theorem. *If an algebra A is neither semi-simple nor nilpotent, and if N is the maximal nilpotent invariant sub-algebra of A, then $A-N$ is semi-simple and has a modulus.*

For, suppose $A-N$ has a nilpotent invariant proper sub-algebra S of index σ. By § 27 (with N in place of B_2), A then has an invariant proper sub-algebra $B_1>N$ such that B_1-N is equivalent to S and hence is nilpotent and of index σ. We recall that the elements of $A-N$ are the classes $[x]$ modulo N, each determined by an element x of A. In particular, let b be an element of B_1. Then class $[b]$ is in B_1-N, whence $[b]^\sigma=[b^\sigma]=[0]$, so that b^σ is in N. Let α be the index of the nilpotent algebra N. Then $b^{\sigma\alpha}=0$, and B_1 is nilpotent, contrary to the definition of N.

If $A-N$ has no modulus, it is a zero algebra Z of order 1 (§ 37), whence $Z^2=0$. Then, if x be any element of A, $[x^2]=[x]^2=[0]$, so that x^2 and hence also x would be nilpotent, whereas A is not nilpotent.

39. Theorem. *A semi-simple algebra A, which is not simple, is reducible.*

For, A has an invariant proper sub-algebra B and has a modulus by Theorem 2 of § 37. Hence $AB=B=BA$. Suppose that B has a nilpotent invariant sub-algebra $I\leqq B<A$. Evidently BIB is invariant in A; it is a proper sub-algebra since $BIB\leqq IB\leqq I$. Thus BIB is o or nilpotent. But A is semi-simple and has no nilpotent invariant proper sub-algebra. Hence $BIB=0$.

Since A has a modulus, AIA is not zero and is evidently invariant in A. Also, $AIA\leqq ABA=BA=B<A$. Thus

$$(AIA)^3=AIA\cdot I\cdot AIA\leqq BIB=0.$$

Hence AIA is a nilpotent invariant proper sub-algebra of A, whereas A is semi-simple. This contradiction proves that B has no nilpotent invariant sub-algebra and (§ 36) hence has a modulus. Our theorem now follows from § 22.

40. Theorem. *A semi-simple algebra A, which is not simple, is a direct sum of simple algebras no one a zero algebra of order* 1, *and conversely.*

For, A has a modulus and by §§ 39, 24 is a direct sum of irreducible algebras A_i each having a modulus (and hence not a zero algebra of order 1). By the proof in § 39 with $B=A_i$, A_i is semi-simple. Since A_i is irreducible, it is simple (§ 39).

Conversely, if each A_i is simple and is not a zero algebra of order 1, then $A=A_1\oplus A_2\oplus\ \ldots\ .$ is semi-simple. For, if I is an invariant sub-algebra of A, then $I=I_1\oplus I_2\oplus\ \ldots\ .$, where $I_j\leqq A_j$. Since

$$AI=A_1I_1+A_2I_2+\ \ldots\ .\leqq I,$$

we have $A_jI_j \leqq I_j$. Similarly, $I_jA_j \leqq I_j$. Hence I_j is invariant in the simple algebra A_j and hence is zero or A_j. Let I be nilpotent and of index a. Then $0 = I^a = \Sigma I_j^a$. Hence each I_j is nilpotent, while A_j is not. Thus $I = 0$.

41. Theorem. *If e is an idempotent element of a semi-simple algebra A, then eAe is semi-simple.*

Since $(eAe)^2 = e \cdot AeA \cdot e \leqq eAe$, eAe is an algebra containing $eee = e$, which is a modulus of it. Suppose it is not semi-simple, but has a nilpotent invariant (proper) sub-algebra N. Since N is invariant in eAe, which has the modulus e, $N \cdot eAe = N$. Hence

$$NAN = Ne \cdot A \cdot eN = NeAe \cdot N = N^2,$$
$$N^rAN = N^{r-1} \cdot NAN = N^{r+1}.$$

Since A has a modulus by Theorem 2 of § 37, $A^2 = A$. Thus

$$(ANA)^2 = ANANA = AN^2A,$$
$$(ANA)^3 = A \cdot N^2AN \cdot A = AN^3A,$$

and, by induction, $(ANA)^r = AN^rA$. Since N is nilpotent, we see that, for r sufficiently large, $(ANA)^r = 0$. Since A has a modulus, ANA contains N and hence is not zero. Thus ANA is a nilpotent invariant sub-algebra of A. This is impossible, since A is semi-simple and not nilpotent.

COROLLARY. *If A is simple, also eAe is simple.*

For, if N is invariant in eAe, which has the modulus e,

$$eANAe = eAe \cdot N \cdot eAe \leqq N < eAe, \qquad ANA < A.$$

Thus ANA is an invariant proper sub-algebra of A, which is impossible since A is simple.

42. Primitive idempotent elements. An idempotent element e of an algebra A is called *primitive* if there exists in A no idempotent element $u(u \neq e)$ for which $eu = u = ue$.

LEMMA. *An idempotent element e of A is primitive if and only if eAe contains no idempotent element $\neq e$.*

For, if $u = eae \neq e$ is idempotent, where a is in A, then $eu = u = ue$, so that e is not primitive for A. Conversely, if e is not primitive, so that A contains an idempotent element $u \neq e$ such that $eu = ue = u$, then eAe contains the idempotent element $eue = u \neq e$.

For example, let $A = (u_1, u_2)$, where $u_1^2 = u_1$, $u_2^2 = u_2$, $u_1 u_2 = 0 = u_2 u_1$. If $\alpha u_1 + \beta u_2$ is idempotent, it is equal to its square $\alpha^2 u_1 + \beta^2 u_2$, whence $\alpha = 0$ or 1, $\beta = 0$ or 1. Hence the only idempotent elements are u_1, u_2 and the modulus $m = u_1 + u_2$ of A. Now m is not primitive, since A contains idempotent elements $u_i \neq m$ having m as modulus (or since $mAm = A$ has idempotent elements $u_i \neq m$). But u_1 is primitive, since $u_1 u_2 = 0 \neq u_2$, $u_1 m = u_1 \neq m$ [or since $u_1 A u_1 = (u_1)$ has no idempotent except u_1]. Similarly, u_2 is primitive. By § 34, m is the only principal idempotent.

THEOREM 1. *If an algebra A contains an idempotent element, it contains at least one primitive idempotent element.*

For, if A contains an idempotent element e which is not primitive, the lemma shows that eAe contains an idempotent element $u \neq e$. Since e is a modulus for eAe, $eu = ue = u$, whence

$$uAu = e \cdot uAu \cdot e \leqq eAe.$$

Here the equality sign is excluded since

$$u(e-u)u=(u-u)u=0, \qquad u\cdot eAe\cdot u<eAe,$$

by Lemma 3 of § 18. Also, $uAu\neq 0$ since $u^3=u\neq 0$. Hence uAu is a proper sub-algebra of eAe.

If the idempotent element u of A is not primitive, the lemma shows that uAu contains an idempotent element $v\neq u$ such that (by the preceding argument) vAv is a proper sub-algebra of uAu. Since the orders of the algebras eAe, uAu, vAv, ... form a series of decreasing positive integers, the process terminates and leads to a primitive idempotent element of A.

In the preceding example, m is not primitive, but is the sum of two primitive idempotent elements u_1 and u_2 such that $u_1u_2=0=u_2u_1$. This illustrates the following

THEOREM 2. *A non-primitive idempotent element e of A is a sum of primitive idempotent elements whose products in pairs are all zero.*

For, by the proof of Theorem 1, $P=eAe$ contains an idempotent element e_1 which is primitive for A, whence $e_1\neq e$. Note that $e^2=e$ is in P and is a modulus for P. Thus $d=e-e_1$ is in P and $de_1=0$, $e_1d=0$. Since $d^2=(e-e_1)d=d$, d is idempotent. Also, $dAd<P$ by the proof of Theorem 1 with u replaced by d. If d (like e_1) is primitive for A, the theorem is proved, since $e=e_1+d$, $e_1d=de_1=0$.

But if d is not primitive for A, a repetition of the argument shows that dAd contains an idempotent element e_2 which is primitive for A, such that $d_1=d-e_2$ is idempotent, $d_1e_2=0=e_2d_1$, and $d_1Ad_1<dAd<P$. Thus $e=e_1+e_2+d_1$. Multiplying this on the right and left by d_1 and e_1 in turn and recalling that d_1 and e_1 are in P, which

has e as a modulus, we find that $d_1 = e_1 d_1 + d_1^2$ or $e_1 d_1 = 0$, $d_1 e_1 = 0$, $e_2 e_1 = 0$, $e_1 e_2 = 0$. Hence all products of e_1, e_2, d_1 in pairs are zero. If d_1 (like e_1 and e_2) is primitive for A, the theorem is proved.

If d_1 is not primitive for A, we argue with d_1 as we did with d. But the series of algebras eAe, dAd, $d_1 A d_1$, ... of decreasing orders must terminate.

Remark. If $u_1, \ldots, u_p$ are $p \geqq 2$ idempotent elements all of whose products in pairs are zero, their sum s is idempotent, but not primitive. For, each u_j has s as a modulus and is distinct from s, since $u_j = s$ implies $0 = u_i u_j = u_i s = u_i (i \neq j)$.

THEOREM 3. *If $u_1, \ldots, u_t$ $(t \geqq 1)$ are primitive idempotent elements of A all of whose products in pairs are zero, and if $e = \Sigma u_i$ is not a principal idempotent element of A, there exists in A a principal idempotent element which is the sum of more than t primitive idempotent elements all of whose products in pairs are zero.*

For, by the theorem of § 34, A contains a principal idempotent element $e+v$, where v is idempotent and $ev = ve = 0$. Evidently $eu_i = u_i = u_i e$, whence $u_i = eu_i e$ is in the algebra eAe. But $v \cdot eAe = ve \cdot Ae = 0$ and similarly $eAe \cdot v = 0$, whence $vu_i = 0 = u_i v$. Hence the theorem is proved if v is primitive. In the contrary case, we know by Theorem 2 that $v = v_1 + \ldots + v_r$, where $v_1, \ldots, v_r (r > 1)$ are primitive idempotent elements of A all of whose products in pairs are zero. Evidently $v_j v = v_j = v v_j$, whence $v_j = v v_j v$ is in the algebra vAv. But $u_i \cdot vAv = 0$, $vAv \cdot u_i = 0$, since $u_i v = 0 = v u_i$. Hence $u_i v_j = 0$, $v_j u_i = 0$.

By combining the case $t = 1$ of this theorem with Theorem 1, we obtain the important

COROLLARY. *Every algebra which is not nilpotent contains a principal idempotent element which is either primitive or a sum of primitive idempotent elements all of whose products in pairs are zero.*

For the example above, m is a principal idempotent element and is not primitive, but is the sum of the primitives u_1 and u_2, for which $u_1u_2=0=u_2u_1$. For the algebra $(1, i)$ over the field of reals, $e^2=e$ implies $e=0$ or 1, whence 1 is the only idempotent and it is therefore both principal and primitive.

CHAPTER V

DIVISION ALGEBRAS

It was proved in § 11 that the algebra of real quaternions has the property that each of the two kinds of division (except by zero) is always possible and unique. Algebras having this property are called division algebras; they play a leading rôle in the general theory of algebras as well as in their arithmetics. We shall prove very simply that the only division algebras over the field of all real numbers are that field, the field of complex numbers, and the algebra of real quaternions. We shall also exhibit a remarkable division algebra of order n^2 over any field.

43. Criteria for a division algebra. An algebra A with a modulus e is called a *division algebra* if every element $a \neq 0$ has in A both a right-hand inverse and a left-hand inverse, viz., elements x and y of A such that $ax = e$, $ya = e$. By Theorem 5, $y = x$.

As noted above, the algebra of real quaternions is a division algebra. The same is true of the algebra (e) of order 1 over any field F, where $e^2 = e$, since either inverse of $a = ae$ is $a^{-1}e$ if a is any number $\neq 0$ of F.

THEOREM 1. *If an algebra A has a single idempotent element e, an element $a \neq 0$, which does not have a right-hand (or left-hand) inverse with respect to e, is properly nilpotent.*

For, the linear set aA (or Aa) is 0 or a sub-algebra of A not containing e, since no element x makes $ax = e$

(or $xa=e$), and hence has no idempotent element and is nilpotent (§ 31). Thus a is properly nilpotent (§ 32).

THEOREM 2. *If A has a single idempotent element e and no properly nilpotent element, then A is a division algebra with the modulus e.*

For, the unique idempotent element e is a principal idempotent by definition (§ 34). Thus e is the modulus of A by the corollary in § 35. Hence A is a division algebra by Theorem 1.

THEOREM 3. *If e is a primitive element of a semi-simple algebra A, then $P=eAe$ is a division algebra.*

For, by the lemma in § 42, P has no idempotent element $\neq e$, while P is semi-simple (§ 41). Hence P is a division algebra by Theorem 2.

Since $P=A$ if e is the modulus of A, we deduce

COROLLARY 1. *If a semi-simple algebra has a modulus, but has no further idempotent element, it is a division algebra.*

If $x\neq 0$, $y\neq 0$, and $xy=0$, x and y are called *divisors of zero*, x being a left-hand divisor and y a right-hand divisor of zero. This is illustrated by the matrices

$$x=\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}, \qquad y=\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}, \qquad xy=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}=0.$$

THEOREM 4. *If A is a division algebra, it contains no divisors of zero, and conversely.*

First, if a division algebra A, with the modulus e, contained elements $x\neq 0$, $y\neq 0$ such that $xy=0$, there would exist an element z of A for which

$$yz=e, \qquad 0=xy\cdot z=x\cdot yz=xe=x.$$

Conversely, let an algebra A contain no divisor of zero. Then A contains no nilpotent element $x\neq 0$,

since $x^a=0$ and $x^{a-1}\neq 0$ imply $x\cdot x^{a-1}=0$. Hence (§ 36) A has a modulus m. If A contains another idempotent element e, the product of e by $m-e$ is zero, while each factor is not zero. Thus A is a division algebra by Theorem 2.

COROLLARY 2. *A division algebra has no nilpotent element $\neq 0$ and hence is semi-simple, and contains no idempotent element other than the modulus.*

This is the converse of Corollary 1.

COROLLARY 3. *Every sub-algebra of a division algebra A is itself a division algebra whose modulus is that of A.*

THEOREM 5. *In a division algebra the two inverses of an element $a\neq 0$ are identical.*

For, $ax=e$ implies $x(ax)a=xea=xa$, whence xa is equal to its square. If $xa=0$, $0=(xa)x=xe=x\neq 0$. Hence xa is idempotent, so that $xa=e$ by Corollary 2. This and $ya=e$ imply $(y-x)a=0$, $y-x=0$.

44. Polynomials in a single element x. Consider an identity

$$f(\omega)g(\omega)\equiv p(\omega) \tag{1}$$

between polynomials in an indeterminate ω with coefficients in a field F. If each polynomial lacks a constant term (free of ω), then (1) implies

$$f(x)g(x)=p(x) \tag{2}$$

for every element x of an associative algebra A over F. For, the term involving ω^k in $f(\omega)g(\omega)$ is obtained by multiplying the term in ω^i of $f(\omega)$ by the term ω^{k-i} of $g(\omega)$ and summing the products for $i=1, \ldots, k-1$. By the associative law, $x^i x^{k-i}=x^k$. Hence (1) implies (2).

Next, let A have the modulus e. If

$$f(\omega)=a_k\omega^k+\ldots+a_1\omega+a_0,$$

we shall write

$$f(x)=a_k x^k+\ \ldots\ .\ +a_1 x+a_0 e\,,$$

in which the constant term a_0 of $f(\omega)$ has been multiplied by e in defining $f(x)$. Under this convention, identity (1) always implies (2).

Since $x^r x^s = x^s x^r$ by the associative law, two polynomials in a single element x are commutative.

45. Real division algebras. Let D be a division algebra of order n over the field $\mathfrak{R}$ of all real numbers. Denote the modulus of D by 1. No discussion is needed for the case $n=1$, since D is then equivalent to $\mathfrak{R}$.

By the theorem in § 6, any $n+1$ elements of D are linearly dependent with respect to $\mathfrak{R}$. In particular, if x is any element of D, then $1, x, x^2, \ldots, x^n$ are dependent, so that x is a root of an equation $p(\omega)=0$ with real coefficients. By the fundamental theorem of algebra, $p(\omega)$ is a product $f_1(\omega)f_2(\omega)\ \ldots$ of linear or quadratic factors with real coefficients. Hence (§ 44) $f_1(x)f_2(x)\ \ldots\ =0$, so that at least one factor is zero by Theorem 4 of § 43. In case that factor is linear, its square is quadratic. Hence every element of D is a root of a quadratic equation with real coefficients.

Let $1, e_1, \ldots, e_{n-1}$ be a set of basal units of D. Then

$$e_i^2+2\rho_i e_i+\sigma_i=0\,, \qquad (e_i+\rho_i)^2=\rho_i^2-\sigma_i\,,$$

where the ρ_i and σ_i are real. Hence after adding a real number to each e_i, we may assume that the square of each new unit e_i is a real number. If the latter were $\geqq 0$, it would be the square of a real number a_i, whence

$$0=e_i^2-a_i^2=(e_i-a_i)(e_i+a_i)=0\,, \qquad e_i=\pm a_i\,,$$

whereas the units 1 and e_i are linearly independent. Hence $e_i^2 = -\beta_i^2$, where β_i is real. Write $E_i = e_i/\beta_i$. Then $E_i^2 = -1$.

If $n = 2$, the algebra $(1, E_1)$ is equivalent to the field of all complex numbers. Henceforth, let $n > 2$, and denote the basal units by $1, I, J, \ldots$, where

$$I^2 = -1, \quad J^2 = -1, \ldots \tag{3}$$

Since $I \pm J$ is a root of a real quadratic equation,

$$(I+J)^2 \equiv -2 + IJ + JI = \alpha(I+J) + \beta,$$
$$(I-J)^2 \equiv -2 - IJ - JI = \gamma(I-J) + \delta,$$

where $\alpha, \beta, \gamma, \delta$ are real numbers. Adding, we get

$$(\alpha+\gamma)I + (\alpha-\gamma)J + \beta + \delta + 4 = 0.$$

Thus $\alpha = \gamma = 0$ since $I, J, 1$ are linearly independent. Hence

$$IJ + JI = 2\epsilon, \quad (I+J)^2 = 2\epsilon - 2, \quad (I-J)^2 = -2\epsilon - 2, \tag{4}$$

where ϵ is a real number. As above, $\pm 2\epsilon - 2 < 0$. Thus $1 - \epsilon^2$ is positive and has a real square root. Write

$$i = I, \quad j = \frac{J + \epsilon I}{\sqrt{1-\epsilon^2}}.$$

Then

$$i^2 = -1, \quad j^2 = -1, \quad ij + ji = 0.$$

The product ij is linearly independent of $1, i, j$ and hence may be taken as the fourth unit k. For, if

$$ij = \lambda + \mu i + \nu j,$$

we multiply by i on the left and get

$$-j = \lambda i - \mu + \nu(\lambda + \mu i + \nu j),$$

whence $-1=\nu^2$, whereas λ, μ, ν were real. Then

$$ij=k, \qquad ji=-k, \qquad k^2=ij(-ji)=i^2=-1.$$

By the associative law,

$$ik=i\cdot ij=-j, \qquad ki=-ji\cdot i=j,$$
$$kj=ij\cdot j=-i, \qquad jk=j(-ji)=i.$$

We have now proved that $1, i, j, k$ are the units of the algebra Q of real quaternions (§ 11).

Finally, let $n>4$. Then D contains a fifth unit l such that $l^2=-1$ and, by the proof which led to (4),

$$il+li=\xi, \qquad jl+lj=\eta, \qquad kl+lk=\zeta,$$

where ξ, η, ζ are real numbers. Then

$$lk=li\cdot j=(\xi-il)j=\xi j-i(\eta-jl)=\xi j-\eta i+kl.$$

Adding lk to each member, we get

$$2lk=\xi j-\eta i+\zeta.$$

Multiplying each term by k on the right, we get

$$-2l=\xi i+\eta j+\zeta k,$$

whereas l is linearly independent of $1, i, j, k$.

THEOREM. *The only division algebras over the field of all real numbers are that field, the field of all complex numbers, and the algebra of real quaternions.*

46. Derivation of division algebras from known ones. For example, consider the field $R(\rho)$ obtained by extending the field R of all rational numbers by the adjunction of a root ρ of a quadratic equation whose coefficients belong to R and which is irreducible in R and has a real root ρ. Then the algebra of quaternions over the real

field $R(\rho)$ is a division algebra which may be regarded as an algebra over R with the eight basal units

$$1,\ \rho,\ i,\ i\rho=\rho i,\ j,\ j\rho=\rho j,\ k,\ k\rho=\rho k.$$

In what precedes we may replace R by any sub-field S of the field of all real numbers for which there is a quadratic equation with coefficients in S, irreducible in S, and having a real root ρ. If that equation is of degree r, we obtain a division algebra over S whose $4r$ basal units are $1,\ \rho,\ \ldots\ ,\ \rho^{r-1}$ and their products by i, j, and k.

Similarly, from each division algebra of order n^2 obtained in the next section we may deduce division algebras of order rn^2.

47. Division algebras of order n^2. We shall define a type of division algebras D of order n^2 over any field F such that they, together with those derived from them by the process of § 46, give all known division algebras other than fields.

By way of introduction, note that if ξ is one root of $\omega^2-s\omega+p=0$, the second root is $\theta(\xi)\equiv s-\xi$, since the sum of the two roots is s. For the same reason, if we subtract the second root from s, we get the first root, whence

$$\theta[\theta(\xi)]=\theta(s-\xi)=s-(s-\xi)=\xi.$$

The first member is denoted by $\theta^2(\xi)$, a notation not to be confused with the square $[\theta(\xi)]^2$ of $\theta(\xi)$.

As a generalization of the quadratic equation, consider an equation $\phi(\omega)=0$ of degree n, with coefficients in a field F, having the roots

$$(5)\qquad \xi,\ \theta(\xi),\ \theta^2(\xi),\ \theta^3(\xi)\equiv\theta[\theta^2(\xi)],\ \ldots\ ,\ \theta^{n-1}(\xi),$$

where $\theta(\xi)$ is a polynomial with coefficients in F such that $\theta^n(\xi)=\xi$. Then if also $\phi(\omega)$ is irreducible in F, we shall call $\phi(\omega)=0$ a *cyclic equation* in F. The case $n=2$ was discussed above. A numerical example for $n=3$ is furnished by (15) below.

Consider the algebra* D over F with the n^2 basal units

$$(6) \qquad y^i x^j \qquad (i,j=0,1,\ldots,n-1),$$

such that

$$(7) \quad \phi(x)=0,\ \phi[\theta(x)]=0,\ \ldots,\ \phi[\theta^{n-1}(x)]=0,\ \theta^n(x)=x,$$

$$(8) \qquad xy=y\theta(x), \qquad y^n=\gamma \qquad (\gamma \text{ in } F).$$

First, let $n=2$, and let F be a field not having the modulus 2. By adding to x a suitably chosen number of F, we may evidently assume that $x^2=\delta$, where δ is in F, but is not the square of a number of F. Then $\theta(x)=-x$, and†

$$(9) \quad D=(1,x,y,yx): \qquad x^2=\delta, \qquad xy=-yx, \qquad y^2=\gamma.$$

The linear functions of x with coefficients in F form an algebra of order 2 equivalent to the field $F(x)$. Hence the general element of D may be designated by $z=u+yv$, where u and v are in $F(x)$. If $v=0$, $u\neq 0$, z has the inverse u^{-1} in $F(x)$. If $v\neq 0$, then $z=wv$, where w is of the form $w=q+y$, where $q=\alpha+\beta x$, with α and β in F. Write $q'=\alpha-\beta x$. Then

$$qy=yq', \qquad (y+q)(y-q')=\gamma-qq'.$$

Hence w has an inverse if $\gamma\neq qq'$.

* Discovered by the author and called a "Dickson algebra" by Wedderburn.

† We may identify D with algebra (18) of § 10 by taking $\alpha=-\delta$, $\beta=-\gamma$, $u_1=x$, $u_2=y$, $u_3=xy$. Then $u_3^2=-x^2y^2=-\alpha\beta$. We saw there that the associative law now yields the complete multiplication table (18). Conversely, since (18) is a matric algebra, it is associative.

THEOREM 1. *For $n=2$, D is a division algebra if γ is not the norm $qq'=\alpha^2-\delta\beta^2$ of a number q of $F(x)$.*

This condition on γ and the foregoing condition that δ is not the square of a number of F are evidently both satisfied when F is the field of all real numbers and γ and δ are both negative. In particular, if $\gamma=\delta=-1$, D is then the algebra of real quaternions and is a division algebra.

For any n, the associative law and (8_1) imply

$$x^2y=xy\theta(x)=y[\theta(x)]^2, \ldots\ldots, x^sy=y[\theta(x)]^s.$$

Multiplication by numbers of F and summation give

$$f(x)y=yf[\theta(x)], \tag{10}$$

for every polynomial f with coefficients in F. By induction,

$$f(x)y^r=y^rf[\theta^r(x)]. \tag{11}$$

Hence, if $f(x)$ and $h(x)$ are any polynomials in x of degree $<n$ with coefficients in F,

$$y^sf(x)\cdot y^rh(x)=y^{s+r}f[\theta^r(x)]h(x). \tag{12}$$

Conversely, it is readily verified that the associative law holds for the algebra D over F for which multiplication is defined by (12) under the agreement that y^{s+r} is to be replaced by γy^{s+r-n} if $s+r\geqq n$, and that the final product fh is found as in ordinary algebra with a subsequent reduction of the degree in x to $n-1$ by use of the equation $\phi(x)=0$ of degree n. In this sense, relations (7) and (8) define an associative algebra D over F with the n^2 units (6).

THEOREM 2. *For $n=3$, D is a division algebra over F if γ is not equal to the norm of any element of the cubic field $F(x)$.*

Here the norm of $f(x)$ means $f(x)f(\theta)f(\theta^2)$, where $\theta^2=\theta[\theta(x)]$.

First, $l=y\lambda(x)+\mu(x)$ has an inverse if it is not zero. For, if $\lambda(x)=0$, $\mu(x)$ is not zero and has an inverse in the field $F(x)$. If $\lambda(x)\neq 0$, it has an inverse. Write $k(x)$ for $-\mu\lambda^{-1}$. Then $l=(y-k)\lambda$ will have an inverse if $y-k$ has one. By (11) and (8_2),

$$[y-k(x)]\,[y^2+yk(\theta^2)+k(\theta)k(\theta^2)]=\gamma-k(x)k(\theta)k(\theta^2)$$

is a number $\neq 0$ of F, so that $y-k$ has an inverse.

Second, we are to prove that $z=y^2+y\alpha(x)+\beta(x)$ has an inverse. Write $w=y-\alpha(\theta)$. Then, by (11), (8_2), and $\theta^3(x)=x$,

$$wz=y\rho+\sigma\,,\qquad \rho=\beta(x)-\alpha(\theta^2)\alpha(x)\,,\qquad \sigma=\gamma-\alpha(\theta)\beta(x)\,.$$

If $\rho=\sigma=0$, then $\gamma=\alpha(\theta)\alpha(\theta^2)\alpha(x)$ would be the norm of $\alpha(\theta)$. Hence $y\rho+\sigma$ is not zero and has an inverse v by the first case. Then $v\cdot wz=1$, so that z has the inverse vw.

48. Division algebras of order 9. To show that there actually exist division algebras of order 9 of the foregoing type D, note that any seventh root $\neq 1$ of unity satisfies the equation

$$\frac{\zeta^7-1}{\zeta-1}=\zeta^6+\zeta^5+\zeta^4+\zeta^3+\zeta^2+\zeta+1=0. \tag{13}$$

Dividing the terms by ζ^3 and rearranging, we get

$$\zeta^3+\frac{1}{\zeta^3}+\zeta^2+\frac{1}{\zeta^2}+\zeta+\frac{1}{\zeta}+1=0.$$

Making the substitution

$$(14)\quad \zeta+\frac{1}{\zeta}=\xi, \qquad \zeta^2+\frac{1}{\zeta^2}=\xi^2-2, \qquad \zeta^3+\frac{1}{\zeta^3}=\xi^3-3\xi,$$

we get

$$(15)\qquad \xi^3+\xi^2-2\xi-1=0.$$

If ϵ is a root $\neq 1$ of $\zeta^7=1$, also ϵ^2 and ϵ^4 are roots of it and hence of (13). By (14), the roots of (15) are

$$\xi_1=\epsilon+\frac{1}{\epsilon}, \qquad \xi_2=\epsilon^2+\frac{1}{\epsilon^2}=\xi_1^2-2, \qquad \xi_3=\epsilon^4+\frac{1}{\epsilon^4}=\xi_2^2-2,$$

while

$$\xi_1=\epsilon^8+\frac{1}{\epsilon^8}=\xi_3^2-2.$$

Hence, in accord with (5), the roots of (15) are

$$\xi_1=\xi, \qquad \xi_2=\theta(\xi)\equiv\xi^2-2, \qquad \xi_3=\theta(\xi_2)=\theta[\theta(\xi)]\equiv\theta^2(\xi),$$

while $\theta(\xi_3)=\theta^3(\xi)=\xi$. Hence (15) will be a cyclic equation for the field R of all rational numbers if it is shown to be irreducible in R. But if the function (15) were reducible, it would have a linear factor $\xi-r$, where r is in R and hence is the quotient a/b of two integers without a common factor >1. Since $r=a/b$ would be a root of (15)

$$\frac{a^3}{b}=-a^2+2ab+b^2$$

would be an integer. But a^3 has no factor >1 in common with b. Hence $b=\pm 1$, $r=\pm a$. Since r is therefore an integral root of (15),

$$r^3+r^2-2r=1,$$

so that r must divide 1, whence $r=\pm 1$. By trial, neither $+1$ nor -1 is a root. Hence (15) is irreducible in R.

Our next step is to compute the norm $N(f)$ of a polynomial $f(\xi_1)$ with rational coefficients. Let m denote their positive least common denominator. Then $f(\xi_1)$ is equal to the quotient of

$$\zeta(\xi_1)=p\xi_1^2+q\xi_1+r$$

by m, where p, q, r, m are integers having no common divisor >1. Thus

$$m^3N(f)=N(\zeta)=\zeta(\xi_1)\zeta(\xi_2)\zeta(\xi_3). \tag{16}$$

The last product will be obtained from the constant term of the cubic equation having the roots $\zeta(\xi_1)$, $\zeta(\xi_2)$, $\zeta(\xi_3)$. This cubic will be found by a simple device.

When ξ is any root of (15), we seek the cubic satisfied by

$$\zeta=p\xi^2+q\xi+r.$$

From $\xi\zeta$ we eliminate ξ^3 by means of (15) and get

$$\xi\zeta=(q-p)\xi^2+(r+2p)\xi+p.$$

Similarly,

$$\xi^2\zeta=(r+3p-q)\xi^2+(2q-p)\xi+q-p.$$

Transposing the left members, we conclude that the determinant of the new coefficients of 1, ξ, ξ^2 is zero:

$$\begin{vmatrix} r-\zeta & q & p \\ p & r+2p-\zeta & q-p \\ q-p & 2q-p & r+3p-q-\zeta \end{vmatrix} =0.$$

Its expansion is of the form $-\zeta^3+ \ldots . +N(\zeta)=0$. Hence $N(\zeta)$ is the value of the preceding determinant for $\zeta=0$, whence

$$N(\zeta)=p^3-2p^2q+6p^2r-pq^2-pqr+5pr^2+q^3-2q^2r-qr^2+r^3.$$

Since $-p\equiv+p\equiv p^2\equiv p^3 \pmod 2$, etc., we have

$$\begin{aligned} N(\zeta) &\equiv p+pq+pqr+pr+q+qr+r \\ &\equiv 1+(p+1)(q+1)(r+1) \pmod 2. \end{aligned}$$

Hence if any one of p, q, r is $\equiv 1$, then $N(\zeta)\equiv 1 \pmod 2$. But if p, q, r are all even, and hence m is odd, $N(\zeta)$ is divisible by 8 since each of its terms is of the third degree in p, q, r. Hence, by (16), $N(f)$ is never equal to an even integer not divisible by 8.

THEOREM. *If γ is an even integer not divisible by 8, the algebra over the field of rational numbers defined by*

$$x^3+x^2-2x-1=0, \qquad xy=y(x^2-2), \qquad y^3=\gamma,$$

is a division algebra of order 9.

49. Summary. We have obtained non-commutative division algebras of orders 4, 8, and 9, each over appropriate fields. It is proved in Appendix II that, besides these and fields, there are no further types of division algebras of order $\leqq 9$. It is shown in Appendix I that the algebra defined by (7) and (8) is a division algebra for every n when γ is suitably restricted.

CHAPTER VI

STRUCTURE OF ALGEBRAS

We shall prove Wedderburn's important theorem that every simple algebra is the direct product of a division algebra and a simple matric algebra, and conversely. Also general theorems on the structure of any algebra which are needed in particular for the proof of the principal theorem on algebras (chap. viii).

50. Direct product. If B and M are linear sets of an algebra such that every element of B is commutative with every element of M and such that the order of the product BM is equal to the product of the orders of B and M, then BM is called the *direct product* of B and M and designated by either $B \times M$ or $M \times B$. We assume henceforth that B and M are algebras. Then $BM \cdot BM = B^2M^2 \leqq BM$, whence $B \times M$ is an algebra.

The elements of $B \times M$ can be expressed as linear combinations of the basal units of M whose coefficients are arbitrary elements of B, or vice versa.

For example, the direct product of the algebra $(1, i, j, k)$ of real quaternions and the real algebra $(1, \sqrt{-1})$ can be expressed as the algebra of complex quaternions.

Since every element of $A = B \times M$ can be expressed as a sum of products of an element of B by an element of M, A has the modulus bm if B and M have the moduli b and m.

As in the example, suppose that B and M are subalgebras of A and have the moduli b and m, respectively. Then the latter coincide with the modulus $a=bm$ of A. For,

$$a-m=a(a-m)=bm(bm-m)=b^2m^2-bm^2=bm-bm=0,$$

whence $m=a$. Similarly, $mb(mb-b)=0$, whence $b=a$.

51. Structure of simple algebras. Let A be a simple algebra over a field F such that A is neither a division algebra nor a zero algebra of order 1. By Theorem 2 of § 37, A has a modulus u. By Theorem 3 of § 43, u is not a primitive idempotent element of A. Hence by Theorem 2 of § 42,

$$u=u_1+\ldots.+u_n \qquad (n\geqq 2), \tag{1}$$

where $u_1, \ldots., u_n$ are primitive idempotent elements all of whose products in pairs are zero. For brevity, write

$$A_{ij}=u_iAu_j.$$

Evidently Au_jA is invariant in A and is not zero since it contains u_j, and hence coincides with the simple algebra A. Thus

$$A_{ij}A_{jk}=u_i\cdot Au_jA\cdot u_k=u_iAu_k=A_{ik},$$

$$A_{ij}A_{hk}=0(j\neq h), \qquad A_{ij}A_{jk}=A_{ik}. \tag{2}$$

Next, $A=\Sigma A_{ij}$ since

$$A=uAu\leqq\Sigma A_{ij}\leqq A.$$

To prove that *the linear sets A_{ij} are supplementary in their sum A*, suppose that A_{rs} has an element $\neq 0$ in common with the sum of the remaining A_{ij}:

$$u_r x u_s = \Sigma u_i x_{ij} u_j \qquad (x, x_{ij} \text{ in } A),$$

summed for $i, j = 1, \ldots, n$ with $[i, j] \neq [r, s]$. Then, multiplying by u_r on the left and by u_s on the right, we get $u_r x u_s = 0$.

By Theorem 3 of § 43, $A_{ii} = u_i A u_i$ is a division algebra with the modulus u_i. Since $A_{ij} A_{ji} = A_{ii} \neq 0$, each $A_{ij} \neq 0$. For $i \neq j$, $A_{ij}^2 = 0$, so that A_{ij} is a zero algebra.

LEMMA 1. *If x_{ij} is any element of A_{ij}, then $P = x_{ij} A_{ji}$ is zero or A_{ii}.*

For, by (2), $A_{ij} A_{ji} = A_{ii}$, whence $P \leqq A_{ii}$. Also, by (2),

$$P A_{ii} = x_{ij} \cdot A_{ji} A_{ii} = x_{ij} A_{ji} = P.$$

If $P \neq 0$, let $p \neq 0$ and x be any elements of P and A_{ii}, respectively, whence px is in $P A_{ii} = P$. If $P < A_{ii}$, and if n is in A_{ii}, but not in P, then $px = n$ is not solvable for x contrary to the fact that A_{ii} is a division algebra.

A similar proof gives

LEMMA 2. *If x_{ij} is any element of A_{ij}, then $A_{ji} x_{ij}$ is zero or A_{jj}.*

LEMMA 3. *If x_{ij} and x_{jk} are elements $\neq 0$ of A_{ij} and A_{jk}, respectively, then $x_{ij} x_{jk} \neq 0$.*

For, suppose that the product is zero. Then

$$x_{jk} A_{kj} = 0, \tag{3}$$

since otherwise $x_{jk} A_{kj} = A_{jj}$ by Lemma 1, whence A_{kj} would contain an element x_{kj} for which

$$x_{jk} x_{kj} = u_j, \qquad 0 \neq x_{ij} = x_{ij} u_j = x_{ij} x_{jk} x_{kj} = 0.$$

Let y_{kj} be an arbitrary element $\neq 0$ of A_{kj}. By (3), $x_{jk}y_{kj}=0$, $x_{jk}\neq 0$. Hence the argument just made shows that $y_{kj}A_{jk}=0$, whence $A_{kj}A_{jk}=0$. Then, by (2), $A_{kk}=0$, contrary to an earlier result.

From the three lemmas we evidently have

LEMMA 4. *If x_{ij} is any element $\neq 0$ of A_{ij}, then*

$$x_{ij}A_{ji}=A_{ii}, \qquad A_{ji}x_{ij}=A_{jj}. \tag{4}$$

By (4) and Lemma 3 of § 18, A_{ji} has the same order as either A_{ii} or A_{jj}, since Lemma 3, with $k=i$, shows that no element $x_{ji}\neq 0$ of A_{ji} makes $x_{ij}x_{ji}=0$, and similarly no element $y_{ji}\neq 0$ of A_{ji} makes $y_{ji}x_{ij}=0$.

Since the A_{ij} are supplementary in their sum, we have

LEMMA 5. *The n^2 algebras A_{ij} all have the same order t, and A itself is of order tn^2.*

Write e_{ii} for u_i $(i=1, \ldots, n)$. Let $e_{12}, \ldots, e_{1n}$ be elements $\neq 0$ of $A_{12}, \ldots, A_{1n}$, respectively. By (4_1) for $i=1$ and $x_{1j}=e_{1j}$, we have $e_{1j}A_{j1}=A_{11}$. Thus, if $j>1$, A_{j1} contains an element e_{j1} such that

$$e_{1j}e_{j1}=e_{11} \qquad (j=1, \ldots, n), \tag{5}$$

which holds also for $j=1$ since e_{11} is idempotent. Define an element e_{pq} of A_{pq} by

$$e_{pq}=e_{p1}e_{1q} \qquad (p, q=2, \ldots, n; \quad p\neq q). \tag{6}$$

Hence we now have n^2 elements $e_{ij}(i, j=1, \ldots, n)$.

If $j\neq h$, $A_{ij}A_{hk}=0$ by (2_1), whence

$$e_{ij}e_{hk}=0 \qquad (j\neq h). \tag{7}$$

Since $u=\Sigma e_{kk}$ is the modulus of A, and $e_{kk}e_{1j}=0$ for $k>1$ by (7),

$$(8) \qquad e_{1j} = \Sigma e_{kk} e_{1j} = e_{11} e_{1j}, \qquad e_{i1} = e_{i1} \Sigma e_{kk} = e_{i1} e_{11},$$

which also follow from the definition of A_{ij} as $e_{ii} A e_{jj}$.

By their definition above, $e_{1i} \neq 0$, $e_{i1} \neq 0$. By Lemma 3, $e_{i1} e_{1i}$ is not zero; it is an element of A_{ii} by (2_2). By (5) and (8_1),

$$(e_{i1} e_{1i})^2 = e_{i1} \cdot e_{1i} e_{i1} \cdot e_{1i} = e_{i1} \cdot e_{11} e_{1i} = e_{i1} e_{1i},$$

whence $e_{i1} e_{1i}$ is idempotent. Since A_{ii} is a division algebra having the modulus e_{ii}, we have $e_{i1} e_{1i} = e_{ii}$ by Corollary 2 of § 43. Combining this result with (6) and (8), we have

$$(9) \qquad e_{ij} = e_{i1} e_{1j} \qquad (i, j = 1, \ldots, n).$$

We conclude from (9) and (5) that

$$e_{ij} e_{jk} = e_{i1} \cdot e_{1j} e_{j1} \cdot e_{1k} = e_{i1} e_{11} e_{1k} = e_{i1} e_{1k} = e_{ik},$$

$$(10) \qquad e_{ij} e_{jk} = e_{ik}.$$

The n^2 elements e_{ij} are linearly independent* since each is not zero and since they belong to n^2 algebras A_{ij} which are supplementary in their sum.

Since the e_{ij} satisfy relations (7) and (10) and are linearly independent, they are the basal units of an algebra M of order n^2 over F which is equivalent to the algebra of all n-rowed square matrices with elements in F (§ 8, § 9, end). Such an algebra M shall be called a *simple*† *matric algebra* of order n^2.

* Also since $e_{gh} \cdot \Sigma a_{ij} e_{ij} \cdot e_{kl} = a_{hk} e_{gl}$ by (7) and (10), for a_{ij} in F.

† The word "simple" is justified by § 52, and is needed since there are further algebras whose elements are matrices.

To each element a_{11} of A_{11} corresponds the element

$$b = \sum_{i=1}^{n} e_{i1} a_{11} e_{1i} . \tag{11}$$

Conversely, b uniquely determines a_{11} since, by (7) and (10),

$$e_{11} b e_{11} = e_{11} a_{11} e_{11} = a_{11} ,$$

e_{11} being the modulus of A_{11}. This one-to-one correspondence is evidently preserved under addition and scalar multiplication, and also under multiplication since

$$\Sigma e_{i1} a_{11} e_{1i} \cdot \Sigma e_{i1} a'_{11} e_{1i} = \Sigma e_{i1} a_{11} e_{11} a'_{11} e_{1i} = \Sigma e_{i1} (a_{11} a'_{11}) e_{1i} . \tag{12}$$

Hence when a_{11} ranges over A_{11}, the totality of elements (11) form an algebra B equivalent to A_{11}. Hence B is a division algebra. If in (12) we take a'_{11} to be the modulus e_{11} of A_{11}, we see that the modulus $\Sigma e_{ii} = \Sigma e_{i1} e_{11} e_{1i}$ of M is the modulus of B. Since

$$b e_{jk} = e_{j1} a_{11} e_{1k} = e_{jk} b , \tag{13}$$

each element (11) of B is commutative with each element e_{jk} of M. Let $a_{11}^{(1)}, \ldots, a_{11}^{(t)}$ be a set of basal units of A_{11}. By (11), they correspond to elements $b^{(1)}, \ldots, b^{(t)}$ which evidently form a basis of B. Now A is of order tn^2 by Lemma 5. It will follow that A has a basis composed of the tn^2 products $b^{(i)} e_{jk}$ if we prove the latter are linearly independent. But, by (13),

$$\sum_{i,j,k} \delta_{ijk} b^{(i)} e_{jk} = \sum_{i,j,k} \delta_{ijk} e_{j1} a_{11}^{(i)} e_{1k} .$$

If this sum is zero when the δ's are in F, we multiply it on the left by e_{1p} and on the right by e_{q1} and get

$$\sum_i \delta_{ipq} a_{11}^{(i)} = 0, \qquad \delta_{ipq} = 0.$$

Hence A is the direct product of B and M.

At the outset we assumed that A is not a division algebra. If it be such, we may evidently regard A as the direct product of A itself by the algebra M_1 of order 1 whose single unit is the modulus u of A. To each element au of M_1, where a is in the field F, we make correspond the one-rowed matrix (a); hence M_1 is equivalent to the algebra of one-rowed matrices with elements in F.

THEOREM. *Any simple algebra A over a field F, not a zero algebra of order 1, can be expressed* as the direct product of a division algebra B over F and a simple matric algebra M over F.*

The moduli of the sub-algebras B and M of A coincide with the modulus u of A. It may happen that either B or M is of order 1, the single unit being u.

When F is the field of real numbers, all division algebras were found in § 45. Hence we have the

COROLLARY. *Apart from a zero algebra of order 1, every simple algebra over the field of all real numbers is a simple matric algebra, or the direct product of the latter by either the binary algebra equivalent to the field of all complex numbers or by the algebra of all real quaternions, and hence is of order n^2, $2n^2$, or $4n^2$.*

* In a single way in the sense of equivalence. For, if also $A = B_1 \times M_1$, where B_1 is a division algebra and M_1 is a simple matric algebra, then B_1 is equivalent to B, and M_1 with M. The proof communicated by Wedderburn to the author is too long to insert here.

52. Converse theorem. *If A is the direct product of a division algebra B over F and a simple matric algebra M over F, then A is a simple algebra over F, not a zero algebra of order* 1.

For, M has a set of basal units e_{ij} satisfying relations (7) and (10). Let D be any invariant sub-algebra of A, and d any element $\neq 0$ of D. Then $d=\Sigma b_{ij}e_{ij}$, where the b_{ij} are elements of B. Let b denote the modulus of B. Since each element of B is commutative with each element of M, the invariant sub-algebra D contains

$$be_{pq}\cdot d\cdot be_{rs}=\sum_{i,j} bb_{ij}be_{pq}e_{ij}e_{rs}=b_{qr}e_{ps}\,.$$

Hence D contains $b_{qr}M$. Since $d\neq 0$, we may choose q and r so that $b_{qr}\neq 0$. Given any element b' of the division algebra B, we can find an element x of it such that $xb_{qr}=b'$, whence $Bb_{qr}=B$. Since D is invariant in A and contains $b_{qr}M$, it contains

$$Bm\cdot b_{qr}M=Bb_{qr}\cdot mM=BM=A\,,$$

where $m=\Sigma e_{ii}$ is the modulus of M. Hence $D=A$, so that A is simple.

Moreover, *an element x of A is commutative with every element of M if and only if x belongs to the sub-algebra Bm.*

For, $x=\Sigma b_{ij}e_{ij}$, where each b_{ij} is in B. Then

$$e_{pq}x=\sum_{i,j} e_{pq}e_{ij}b_{ij}=\sum_{j} e_{pj}b_{qj}\,,\qquad xe_{pq}=\sum_{i} e_{iq}b_{ip}\,.$$

These sums are equal for all values of p and q if and only if $b_{qq}=b_{pp}$ (by the coefficients of e_{pq}) and $b_{qj}=0 (j\neq q)$, whence $x=b_{11}\Sigma e_{ii}=b_{11}m$.

The special case $B=(b)$ of the theorem and this supplement shows that *M is simple and that an element of M which is commutative with every element of M is a scalar multiple of its modulus m.*

The special case $M=(m)$ shows that *any division algebra B is simple.**

53. Idempotent elements of a difference algebra. Let A be an algebra, over the field F, which is neither nilpotent nor semi-simple. Thus A has a maximal nilpotent invariant proper sub-algebra N. By § 38, $A-N$ is semi-simple and has a modulus. Write $[x]$ for the class, containing x, of A modulo N.

THEOREM 1. *If e is an idempotent element of A, then $[e]$ is an idempotent class of $A-N$.*

For, $[e]^2=[e^2]=[e]$ and $[e]\neq[0]$ since e is not in N.

THEOREM 2. *Every idempotent class $[u]$ of $A-N$ contains idempotent elements of A.*

For, $[0]\neq[u]=[u^2]=\ \ldots\ =[u^r]$. Hence $u^r\neq 0$ for every positive integer r, so that u is not nilpotent. The linear set $S=(u,\ u^2,\ \ldots)$ is evidently closed under multiplication and hence is an algebra. But S is not nilpotent since u is not, and hence contains an idempotent element e (§ 31). Thus

$$e=a_1u+a_2u^2+\ \ldots\ +a_hu^h \qquad (a_i \text{ in } F),$$

$$[e]=a_1[u]+\ \ldots\ +a_h[u^h]=a[u], \qquad a=a_1+\ \ldots\ +a_h.$$

$$a[u]=[e]=[e]^2=a^2[u]^2=a^2[u], \qquad a=a^2.$$

But $a=0$ would imply $[e]=[0]$ and hence that e is nilpotent, whereas it is idempotent. Hence $a=1$, $[e]=[u]$, so that e is an idempotent element of A belonging to $[u]$.

* To give a direct proof, let $b'\neq 0$ and b_1 be any elements of B. There exists an element x of B such that $xb'=b_1$. Hence if b' belongs to any invariant sub-algebra D, also $xb'=b_1$ belongs to D, whence $D=B$.

THEOREM 3.* *If u is a primitive idempotent element of A, then $[u]$ is a primitive idempotent element of $A-N$.*

In view of the lemma in § 42, it suffices to prove that, if $[v]$ is any idempotent element of $[u]\ (A-N)\ [u]$, then $[v]$ coincides with $[u]$. We have

$$[v]=[u]\,[x]\,[u]=[uxu],$$

where x is in A. By the proof of Theorem 2, the algebra

$$Y=(y,\ y^2,\ \ldots .), \qquad y=uxu,$$

contains an idempotent element w of A belonging to $[y]$. Since y is an element of uAu, the element w of Y is in uAu. By the hypothesis that u is primitive, $w=u$. Hence

$$[v]=[y]=[w]=[u].$$

THEOREM 4. *If e is a principal idempotent element of A, then $[e]$ is a principal idempotent element of $A-N$ and is identical with its modulus.*

For, in the decomposition of A relative to e,

$$A=I+eR+Le+eAe,$$

each element of the first three parts is o or properly nilpotent by the corollary in § 35, and hence is in N. Hence we obtain all classes $[x]$ of $A-N$ by restricting x to eAe. Each element of $A-N$ is therefore of the

* We make no use of the converse that if u is an idempotent of A such that $[u]$ is a primitive idempotent element of $A-N$, then u is a primitive of A. For, if $v=uxu$ is an idempotent of uAu, $[v]$ is one of $[u]\ (A-N)\ [u]$ and coincides with the given primitive idempotent $[u]$ of $A-N$. Thus $u-v$ is in N. But $u-v$ is equal to its square. Hence $u-v=0$.

form $[e]\,[a]\,[e]$, whence $[e]$ is the modulus of $A-N$ and therefore a principal idempotent of it (§ 34).

54. Condition for a simple matric sub-algebra.

THEOREM. *If A has the maximal nilpotent invariant sub-algebra N and if $A-N$ contains a simple matric algebra M, then A contains a sub-algebra equivalent to M.*

By hypothesis, M has the basal units $[\epsilon_{ij}]$, each a class of A modulo N, such that

$$(14)\quad [\epsilon_{ij}]\,[\epsilon_{jk}]=[\epsilon_{ik}],\quad [\epsilon_{ij}]\,[\epsilon_{lk}]=0 \qquad (j\neq l;\ i,j,l,k=1,\ \ldots\ldots,\ n).$$

The class $[\epsilon_{11}]$ contains an idempotent element e_{11} of A by Theorem 2 of § 53 or by (18) with $r=1$. We shall prove that *A contains idempotent elements $e_{11},\ \ldots\ldots,\ e_{nn}$ all of whose products in pairs are zero, and such that e_{ii} is in the class $[\epsilon_{ii}]$.*

To prove this by induction on n, let A contain idempotent elements $e_{11},\ \ldots\ldots,\ e_{r-1,\,r-1}$ whose products in pairs are zero and such that e_{ii} is in the class $[\epsilon_{ii}]$. Let s denote the sum of these e_{ii}. Then

$$(15)\qquad e_{ii}s=e_{ii}=se_{ii},\ s^2=s \qquad (i=1,\ \ldots\ldots,\ r-1).$$

Select any element b_r of class $[\epsilon_{rr}]$ and write*

$$a_r=(1-s)b_r(1-s)\equiv b_r-sb_r-b_rs+sb_rs.$$

By (15), we evidently have

$$(16)\qquad e_{ii}a_r=0=a_re_{ii} \qquad (i=1,\ \ldots\ldots,\ r-1).$$

Since s and b_r are in the classes $[\epsilon_{11}]+\ \ldots\ldots+[\epsilon_{r-1,\,r-1}]$ and $[\epsilon_{rr}]$, respectively, whose product in either order is zero by (14), we see that $[a_r]=[b_r]=[\epsilon_{rr}]$. Hence

* The use of the abbreviation $(1-s)b$ for $b-sb$ does not imply that A has a modulus.

$[a_r]^2=[a_r]$, so that $a_r^2-a_r$ is an element z of N, whence $z^a=0$. Evidently z is commutative with a_r. By (16),

$$(17)\qquad e_{ii}z=0=ze_{ii}\qquad (i=1,\ \ldots\ ,\ r-1).$$

Employing series* which stop with the term in z^{a-1}, write

$$(18)\quad e_{rr}=\frac{2a_r-1}{2\sqrt{1+4z}}+\tfrac{1}{2}\equiv a_r(1-2z+12z^2-\ \ldots\ )\\ +z-6z^2+\ \ldots\ .$$

Then $e_{rr}^2=e_{rr}$. By means of (16) and (17), we find that

$$e_{ii}e_{rr}=0=e_{rr}e_{ii}\qquad (i=1,\ \ldots\ ,\ r-1).$$

Since a_rz is in the invariant sub-algebra N, e_{rr} is in the class $[a_r]=[\epsilon_{rr}]$. This completes the proof by induction of the foregoing italicized result.

For $p\neq q$, choose any element t_{pq} of the class $[\epsilon_{pq}]$ and write a_{pq} for $e_{pp}t_{pq}e_{qq}$. Then

$$(19)\qquad e_{pp}a_{pq}e_{qq}=a_{pq}\,,$$
$$[a_{pq}]=[\epsilon_{pp}]\,[\epsilon_{pq}]\,[\epsilon_{qq}]=[\epsilon_{pq}]\,,$$
$$[a_{1r}a_{r1}]=[\epsilon_{1r}]\,[\epsilon_{r1}]=[\epsilon_{11}]=[e_{11}],\qquad [a_{r1}a_{1r}]=[e_{rr}]\,,$$

by (14), so that

$$a_{1r}a_{r1}=e_{11}+z_{1r}\,,\qquad a_{r1}a_{1r}=e_{rr}+z_{2r}\,,$$

where z_{1r} and z_{2r} are in N. From (19), we get

* By the binomial theorem the inverse of $\sqrt{1+4z}$ is

$$(1+4z)^{-\frac{1}{2}}=1-\tfrac{1}{2}(4z)+(-\tfrac{1}{2})(-\tfrac{1}{2}-1)(4z)^2+\ \ldots\ .=1-2z+12z^2-\ \ldots\ .$$

But if the field has the modulus 2, we replace (18) by

$$e_{rr}=a_r+z+z^2+z^4+z^8+\ \ldots\ .$$

$$(20) \qquad e_{pp}a_{pq}=a_{pq}\,, \qquad a_{pq}e_{qq}=a_{pq}\,.$$

Thus $e_{11}a_{1r}a_{r1}=a_{1r}a_{r1}$, $a_{r1}a_{1r}e_{rr}=a_{r1}a_{1r}$, whence

$$(21) \qquad a_{1r}a_{r1}=e_{11}(1+z_{1r})\,, \qquad a_{r1}a_{1r}=(1+z_{2r})e_{rr}\,.$$

By (20) and (21),

$$a_{r1}\cdot a_{1r}a_{r1}=a_{r1}+a_{r1}z_{1r}\,, \qquad a_{r1}a_{1r}\cdot a_{r1}=a_{r1}+z_{2r}a_{r1}\,.$$

Since these are equal by the associative law,

$$(22) \qquad a_{r1}z_{1r}=z_{2r}a_{r1}\,, \qquad a_{r1}z_{1r}^{t}=z_{2r}^{t}a_{r1}\,.$$

If z is N, so that $z^{a}=0$, the product of $a(1+z)$ by

$$(1+z)^{-1}=1-z+z^{2}-\ \ldots\ .\ +(-1)^{a-1}z^{a-1}$$

is a. Hence by (22),

$$(23) \qquad a_{r1}(1+z_{1r})^{-1}=(1+z_{2r})^{-1}a_{r1}\,.$$

For $r>1$, write

$$(24) \qquad e_{1r}=a_{1r}\,, \qquad e_{r1}=a_{r1}(1+z_{1r})^{-1}\,.$$

Then by (21_1) and the case $e_{11}a_{1r}=a_{1r}$ of (20), we get

$$(25) \qquad e_{1r}e_{r1}=a_{1r}a_{r1}(1+z_{1r})^{-1}=e_{11}\,, \qquad e_{11}e_{1r}=e_{1r}\,.$$

Now e_{r1} of (24) is equal to the second member of (23). Hence by the case $a_{r1}e_{11}=a_{r1}$ of (20) and by (21_2), we get

$$(26) \quad e_{r1}e_{11}=(1+z_{2r})^{-1}a_{r1}e_{11}=e_{r1}\,, \qquad e_{r1}e_{1r}=(1+z_{2r})^{-1}a_{r1}a_{1r}=e_{rr}\,.$$

Finally write e_{pq} for $e_{p1}e_{1q}$ when $p>1$, $q>1$, $p\neq q$. This and (25_2) and (26) give

$$e_{ij}=e_{i1}e_{1j} \qquad (i,j=1,\ \ldots\ .\ ,n).$$

By this and (25_1), we get

$$e_{ij}e_{jk}=e_{i1}e_{1j}\cdot e_{j1}e_{1k}=e_{i1}\cdot e_{11}\cdot e_{1k}=e_{i1}e_{1k}=e_{ik}\,.$$

Finally, if $j \neq h$,

$$e_{ij}e_{hk} = e_{i1}e_{1j} \cdot e_{h1}e_{1k} = e_{i1} \cdot e_{1j}e_{jj} \cdot e_{hh}e_{h1} \cdot e_{1k} = 0,$$

since $e_{jj}e_{hh} = 0$. Hence the e_{ij} are basal units of a simple matric sub-algebra of A.

55. Structure of any algebra. By § 40, a semi-simple algebra is either simple or is a direct sum of simple algebras no one of which is a zero algebra of order 1. The structure of each such simple algebra is known by § 51. Hence we know the structure of all semi-simple algebras.

THEOREM. *Let A be an algebra over a field F such that A has a modulus a and is not semi-simple. Hence A has a maximal nilpotent invariant proper sub-algebra N. Suppose* that $A-N$ is simple. Then A is the direct product of a simple matric algebra† M over F by an algebra B over F having a modulus, but no further idempotent element.*

By § 51, $A-N$ is a direct product $[B]\times[M]$, where $[B]$ is a division algebra and $[M]$ is a simple matric algebra, and their moduli coincide with the modulus $[a]$ of $A-N$. By § 54, A contains a sub algebra M equivalent to $[M]$. Denote the basal units of M by e_{ij}. Write $e = \Sigma e_{ii}$. Then

$$e^2 = e, \qquad ea = e = ae, \qquad (e-a)^2 = a-e.$$

By induction,

$$(e-a)^n = (-1)^{n+1}(e-a). \tag{27}$$

* The general case is reduced to this in § 57.

† Any two determinations of M are equivalent by the final footnote in § 51.

This implies $e=a$ since $[e]=[a]$, so that $e-a$ is in N and hence is nilpotent.

Let x be any element of A and write

$$x_{pq}=\Sigma e_{ip}xe_{qi}\,. \tag{28}$$

Then

$$\sum_{p,\,q} x_{pq}e_{pq}=\sum_{p,\,q,\,i} e_{ip}xe_{qi}e_{pq}=\sum_{p,\,q} e_{pp}xe_{qq}=exe=axa=x\,, \tag{29}$$

$$x_{pq}e_{ij}=e_{ip}xe_{qj}=e_{ij}e_{jp}xe_{qj}=e_{ij}x_{pq}\,,$$

so that x_{pq} and e_{ij} are commutative for all values of p, q, i, j. The proof of the second theorem in § 52 shows that x is commutative with every e_{ij} if and only if $x=x_{11}e$. But $e=a$ is the modulus of A. Hence the x_{11} are the elements of a sub-algebra B of A which is composed of all those elements of A which are commutative with every element of M. Thus B has modulus e.

Since every x_{pq} is commutative with each unit e_{ij} of M, it belongs to B. Hence, by (29), every element of A is expressible in the form

$$\Sigma b_{pq}e_{pq} \qquad (b_{pq} \text{ in } B). \tag{30}$$

If two such sums are equal, they are identical. For, their difference can be expressed as such a sum. Hence let (30) be zero. Multiply it on the left by e_{ij} and on the right by e_{ri}, and note that b_{pq} may be permuted with e_{ij}. We get $b_{jr}e_{ii}=0$. Summing as to i, and noting that $e=a$, we get $b_{jr}=0$ for all values of j and r.

Hence $A=B\times M$. Further, we have proved that B and M have the same modulus a as A. Since $[B]$ is a division algebra, it has no idempotent element other than

its modulus by Corollary 2 of § 43. Hence if e is any idempotent element of B, $[e]=[a]$, and we have (27) and therefore $e=a$.

56. If A is semi-simple, its N is zero. Then if $A-N$ is simple, also A is simple. Hence we may combine the preceding theorem with that in § 51 as follows:

THEOREM. *If A has a modulus and $A-N$ is simple, where N is the maximal nilpotent invariant sub-algebra if it exists, but is zero in the contrary case, then A is the direct product of a sub-algebra B having a modulus, but no further idempotent element, by a simple matric sub-algebra M.*

The converse is true. In the proof we may assume that B has a maximal nilpotent invariant sub-algebra N_1, since otherwise B is a division algebra by Theorem 2 of § 43 and A is simple (§ 52), whence the converse holds with $N=0$.

The N of $A=B\times M$ is $N_1\times M$. For, if x is in N, also (28) is in the invariant algebra N and, being also in B, is in N_1 (§ 32). Conversely, if x_{pq} is in N_1 and hence in N, then $\Sigma x_{pq}e_{pq}$ is in N.

Hence $A-N=(B-N_1)\times M$. But $B-N_1$ is semi-simple and its single idempotent element is its modulus; hence it is a division algebra by Corollary 1 in § 43. Thus $A-N$ is simple (§ 52).

57. Let A be any algebra which is neither semi-simple nor nilpotent. Then A has a maximal nilpotent invariant proper sub-algebra N. By the corollary in § 42, A contains a principal idempotent element u which is either primitive (and we then write $u=u_1$) or else is a sum of primitive idempotent elements $u_1, \ldots, u_n$ whose products in pairs are all zero.

The semi-simple algebra $A-N$ is either a simple algebra $(A-N)_1$ or a direct sum of simple algebras

$$(31) \qquad (A-N)_1, \ldots, (A-N)_t.$$

By § 53, the idempotent element $[u]$ of $A-N$ is its modulus and is a sum of primitive idempotent elements $[u_1], \ldots, [u_n]$ of $A-N$ whose products in pairs are all zero.

Each $[u_k]$ belongs to one of the algebras (31). For, if $[u_k]=\Sigma v_i$, where v_i is in $(A-N)_i$, then

$$v_iv_j=0 (i\neq j), \qquad [u_k]=[u_k]^2=\Sigma v_i^2, \qquad v_i=v_i^2.$$

Hence those of the v_i which are not zero are idempotent. But if two or more of the v_i are idempotent, $[u_k]$ would not be primitive by the Remark in § 42.

The subscripts $1, \ldots, n$ may be chosen so that

$[u_1], \ldots, [u_{p_1}]$ belong to $(A-N)_1$,
$[u_{p_1+1}], \ldots, [u_{p_1+p_2}]$ belong to $(A-N)_2$, etc.

Write

$$e_1=u_1+\ldots+u_{p_1}, \quad e_2=u_{p_1+1}+\ldots+u_{p_1+p_2}, \ldots,$$
$$e_t=u_r+\ldots+u_n,$$

where $r=p_1+\ldots+p_{t-1}+1$. Then $e_1, \ldots, e_t$ are idempotent elements of A whose products in pairs are all zero and whose sum is u.

Since $[e_1], \ldots, [e_t]$ belong to the respective algebras (31) and since their sum is the modulus $[u]$ of the direct sum $A-N$ of those algebras, they are the moduli of those algebras (§ 21). Also,

$$(32) \qquad [e_i](A-N)[e_j]=[e_i]\sum_{k=1}^{t}(A-N)_k[e_j]=0 \qquad (i\neq j).$$

In the decomposition of A relative to u (§ 33):

$$A=I+uB+Bu+uAu,$$

the first three linear sets belong to N by the corollary in § 35, whence

$$(33) \qquad A=N_1+uAu, \qquad N_1\leqq N.$$

We shall employ the abbreviations

$$A_{ij}=e_iAe_j, \qquad N_{ij}=e_iNe_j, \qquad N_2=\sum_{i\neq j}N_{ij}.$$

By (32) and the fact that N is invariant in A, we have $e_iAe_j\leqq N(i\neq j)$, so that every element $p=e_iae_j$ of A_{ij} is in N, whence $e_ipe_j=p$, and $A_{ij}=N_{ij}$ $(i\neq j)$. Hence

$$(34) \qquad uAu=\Sigma A_{ij}=N_2+\Sigma A_{ii},$$

$$(35) \qquad A=N'+\Sigma A_{ii}, \qquad N'=N_1+N_2\leqq N.$$

If an element a_j of A_{jj} is properly nilpotent for A_{jj}, it is properly nilpotent also for A. For, by (35), each element x of A is of the form $x'+\Sigma x_i$, where x' is in N' and x_i is in A_{ii}. Since $A_{jj}A_{ii}=0(j\neq i)$, $a_jx=a_jx'+a_jx_j$. Since x' is in the invariant sub-algebra N of A, a_jx' is in N. Hence $[a_jx]=[a_jx_j]$. Since a_j is properly nilpotent for A_{jj}, a_jx_j is nilpotent, and the same is therefore true of class $[a_jx_j]$ and hence of $[a_jx]$. Thus powers of a_jx with sufficiently large exponents are elements of N, whence a_jx is nilpotent. Since x was arbitrary in A, this proves that a_j is properly nilpotent for A.

The same argument* shows that if an element a of uAu is properly nilpotent for it, a is such for A. For, by (34), $a=v+\Sigma a_i$, where v is in N_2 and a_i is in A_{ii}. For x_i in A_{ii}, Σx_i is in uAu, and $a\Sigma x_i=\mu+\Sigma a_i x_i$ is nilpotent, where μ is in N. This sum differs from ax by an element of N. Hence $[ax]$ and therefore ax is nilpotent, whence a is properly nilpotent for A.

Let N_j denote o or the maximal nilpotent invariant sub-algebra of A_{jj}, according as there is not or is such a sub-algebra. As proved above, $N_j \leqq N$. Next, if N_{jj} is not zero, it is a nilpotent invariant sub-algebra of A_{jj}. For, since N is invariant in A,

$$N_{jj} \leqq N, \qquad A_{jj}N_{jj}=e_j \cdot Ae_jN \cdot e_j \leqq e_jNe_j \leqq N_{jj},$$

and similarly $N_{jj}A_{jj} \leqq N_{jj}$. Moreover, $A_{jj} \frown N = N_{jj}$. For, if an element v of N is in A_{jj}, so that $v=e_jae_j$, then $e_jve_j=v$, and v is in N_{jj}. Hence N_{jj} is the foregoing maximal N_j.

Similarly, uNu is the intersection of uAu and N, and is evidently invariant in uAu. Hence uNu is zero or the maximal nilpotent invariant sub-algebra of uAu, according as there is not or is such a sub-algebra.

The distribution of the elements of A_{jj} into classes is the same modulo N_{jj} as modulo N. For, if x and y are elements of A_{jj} belonging to the same class (or different classes) of A modulo N, then $x-y$ is in A_{jj} and is in

* To give another proof, let I be any nilpotent invariant sub-algebra of uAu. Then $I^\beta=0$ for a certain positive integer β. Hence $(I+N)^\beta \leqq N$, since N is invariant in A. Thus $I+N$ is nilpotent. To prove it is invariant in A, use (33). Then

$$A(I+N)=(N_1+uAu)(I+N) \leqq uAu \cdot I+N \leqq I+N.$$

Similarly, $(I+N)A \leqq I+N$. Since $I+N$ is a nilpotent invariant sub-algebra of A, it is contained in N (§ 30). Hence $I \leqq N$.

(or not in) N and therefore is in (or not in) N_{jj}, whence x and y belong to the same class (or different classes) of A_{jj} modulo N_{jj}, and conversely.

The class of A modulo N which is determined by an element e_jxe_j of A_{jj} is

$$[e_j][x][e_j]. \tag{36}$$

Now $[x]$ is in $A-N$ which is the direct sum of algebras (31). Also,

$$[e_j]\Sigma(A-N)_i[e_j]=[e_j](A-N)_j[e_j]=(A-N)_j.$$

Hence (36) is an element of $(A-N)_j$. Conversely, any element of the latter is of the form (36) with x in A, and hence is in a class of A modulo N determined by an element e_jxe_j of A_{jj}. Thus, by the preceding paragraph, $(A-N)_j$ is equivalent to $A_{jj}-N_{jj}$, which is therefore simple. Applying § 56, with A replaced by A_{jj}, we obtain the

THEOREM. *Let A be any algebra which is neither semi-simple nor nilpotent and let N be its maximal nilpotent invariant sub-algebra. Then $A-N$ is a direct sum of t simple algebras ($t\geqq 1$), and A contains a principal idempotent element $u=e_1+\ldots+e_t$, where the e_i are idempotent elements whose products in pairs are all zero. Then $A=N'+S$, where $N'\leqq N$ and S is the direct sum of the t algebras $e_jAe_j(j=1,\ldots,t)$ and each e_jAe_j is the direct product of a simple matric algebra by an algebra having the modulus e_j, but no further idempotent element. Moreover, e_jAe_j (or uAu) has the maximal nilpotent invariant sub-algebra e_jNe_j (or uNu) or no such sub-algebra, according as e_jNe_j (or uNu) is not or is zero. Also, $N=N'+\Sigma e_jNe_j$.*

CHAPTER VII

CHARACTERISTIC MATRICES, DETERMINANTS, AND EQUATIONS; MINIMUM AND RANK EQUATIONS

We shall prove that every associative algebra is equivalent to a matric algebra and apply this result to deduce important theorems on characteristic, minimum, and rank equations from related theorems on matrices. In § 66 we shall establish a criterion for a semi-simple algebra which will be applied both in the proof of the principal theorem on algebras (chap. viii) and in the study of the arithmetics of algebras.

58. Every associative algebra is equivalent to a matric algebra. The essential point in the proof of this equivalence is brought out most naturally by explaining the correspondence, first noted by Poincaré, between the elements of any associative algebra A over a field F and the linear transformations of a certain set (group).

Let the units $u_1, \ldots, u_n$ of A have the multiplication table

$$(1) \qquad u_i u_j = \sum_{k=1}^{n} \gamma_{ijk} u_k \qquad (i, j = 1, \ldots, n).$$

Then A is associative if and only if $u_i(u_s u_r) = (u_i u_s) u_r$ for all values of i, s, r, and hence, by (1), if and only if

$$(2) \qquad \sum_{j=1}^{n} \gamma_{srj}\gamma_{ijk} = \sum_{j=1}^{n} \gamma_{isj}\gamma_{jrk} \qquad (i, s, r, k = 1, \ldots, n).$$

Let x be a fixed element and z, z' variable elements

$$x=\Sigma\xi_i u_i, \qquad z=\Sigma\zeta_k u_k, \qquad z'=\Sigma\zeta'_j u_j$$

of A. By (1), $z=xz'$ is equivalent to the n equations

$$(3) \qquad T_x: \qquad \zeta_k=\sum_{i,j}\xi_i\gamma_{ijk}\zeta'_j \qquad (k=1, \ldots, n),$$

which define a linear transformation T_x from the initial variables $\zeta_1, \ldots, \zeta_n$ to the new variables $\zeta'_1, \ldots, \zeta'_n$. The determinant of T_x is

$$(4) \qquad \Delta(x)\equiv\left|\sum_{i=1}^{n}\xi_i\gamma_{ijk}\right| \qquad (j, k=1, \ldots, n).$$

Given the numbers ζ_k and $\xi_i (k, i=1, \ldots, n)$ of F such that $\Delta(x)\neq 0$, we can find unique solutions ζ'_j of the n equations (3). In other words, there exists a unique element z' of A such that $xz'=z$, when z and x are given and $\Delta(x)\neq 0$.

Similarly, the equation $z'=yz''$ between the foregoing z' and $y=\Sigma\eta_s u_s$, $z''=\Sigma\zeta''_r u_r$, is equivalent to the n equations

$$T_y: \qquad \zeta'_j=\sum_{r,s}\eta_s\gamma_{srj}\zeta''_r \qquad (j=1, \ldots, n),$$

which define a transformation T_y from the variables $\zeta'_1, \ldots, \zeta'_n$ to the final variables $\zeta''_1, \ldots, \zeta''_n$. By eliminating the ζ'_j, we get the equations of the product (§ 2):

$$T_xT_y: \qquad \zeta_k=\sum_{i,j,r,s}\xi_i\eta_s\gamma_{ijk}\gamma_{srj}\zeta''_r \qquad (k=1, \ldots, n).$$

This transformation will be proved to be identical with T_p, where $p=xy$. This becomes plausible by elimination of z' between $z=xz'$ and $z'=yz''$, whence $z=x\cdot yz''=pz''$ by the associative law. To give a formal proof, note that to $p=\Sigma\pi_j u_j$ corresponds the transformation

$$T_p: \qquad \zeta_k=\sum_{j,r}\pi_j\gamma_{jrk}\zeta_r'', \qquad \pi_j\equiv\sum_{i,s}\xi_i\eta_s\gamma_{isj},$$

in which the value of π_j was computed from $p=xy$ by use of (1). Then $T_xT_y=T_p$, since the coefficients of $\xi_i\eta_s\zeta_r''$ are the sums (2).

Hence the correspondence (3) between any element x of the associative algebra A and the transformation T_x has the property that to the product xy of any two elements corresponds the product T_xT_y of the corresponding transformations. Thus the set of these transformations is such that the product of any two of them is one of the set.*

There is a second correspondence between any element x of A and the transformation obtained from $z=z'x$:

$$(5) \qquad t_x: \qquad \zeta_k=\sum_{i,j}\xi_i\gamma_{jik}\zeta_j' \qquad (k=1,\ \ldots\ ,\ n).$$

* Such a set is called a *group* if it contains the identity transformation I and the inverse of each T_x. If A has a modulus e, then $T_e=I$ since $z=ez'=z'$ gives $\zeta_k=\zeta_k'(k=1,\ \ldots\ ,\ n)$. If $\Delta(x)\neq 0$, we saw that there exists a unique element w of A such that $xw=e$. Then $T_xT_w=I$, so that T_w is the inverse of T_x. Hence all the transformations T_x for which $\Delta(x)\neq 0$ form a group. Then also $T_wT_x=I$ and $wx=e$ for a unique w, whence $\Delta'(x)$, defined below (5), is not zero. Conversely, $\Delta'(x)\neq 0$ implies $\Delta(x)\neq 0$ if A has a modulus.

Similarly, from $z'=z''y$ we obtain t_y. Then $z=z''q$, $q=yx$. This makes it plausible that $t_x t_y = t_q$. A formal proof follows from (2) as before. The determinant of (5) is denoted by $\Delta'(x)$. If it is not zero, there exists a unique element z' such that $z'x=z$.

We shall denote the matrix of transformation (3) by R_x and that of (5) by S_x, whence

$$(6) \quad R_x=(\rho_{kj}), \qquad \rho_{kj}=\sum_{i=1}^{n}\xi_i\gamma_{ijk} \qquad (k, j=1, \ldots, n),$$

having the element ρ_{kj} in the kth row and jth column;

$$(7) \quad S_x=(\sigma_{kj}), \qquad \sigma_{kj}=\sum_{i=1}^{n}\xi_i\gamma_{jik} \qquad (k, j=1, \ldots, n).$$

We shall call R_x and S_x the *first* and *second matrices* of x (with respect to the chosen units $u_1, \ldots, u_n$). Since the matrix of a product of two transformations is equal to the product of their matrices (§ 3), we have

$$(8) \qquad R_x R_y = R_{xy}, \qquad S_x S_y = S_{yx}.$$

The determinants $\Delta(x)$ and $\Delta'(x)$ of R_x and S_x are called the *first* and *second determinants* of x (with respect to $u_1, \ldots, u_n$).

Since R_x is the matrix of transformation (3), $R_x=0$ implies that ζ_k is zero identically in the ζ_j', and hence that $0=xz'$ for every z' in A. Similarly, $S_x=0$ implies that $0=z'x$ for every z' in A. In particular,

THEOREM 1. *If A has a modulus, either $R_x=0$ or $S_x=0$ implies $x=0$.*

Since each element of R_x or S_x is linear and homogeneous in the co-ordinates ξ_i of x by (6) or (7), we have

$$R_{\alpha x}=\alpha R_x\,, \qquad R_x+R_y=R_{x+y}\,, \tag{9}$$

for every number α of F, and the similar equations in S.

By (8_1) and (9), the correspondence between elements $x, y, \ldots$ of algebra A and matrices $R_x, R_y, \ldots$ is such that xy, αx, and $x+y$ correspond to R_xR_y, αR_x, and R_x+R_y, respectively. Moreover, if A has a modulus, this correspondence is one-to-one. For, if $R_x=R_y$, then $0=R_x-R_y=R_{x-y}$, whence $x-y=0$ by Theorem 1. Hence by § 12 we have

THEOREM 2. *Any associative algebra A with a modulus is equivalent to the algebra whose elements are the first matrices R_x of the elements x of A, and is reciprocal to the algebra whose elements are the second matrices S_x of the elements x of A.*

For example, let A be the algebra of two-rowed matrices

$$m=\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \mu=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \qquad \mu_1=\begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix}.$$

Then $\mu_1=m\mu$ and $\mu_1=\mu m$ lead to transformations T_m on the variables $\alpha, \gamma, \beta, \delta$, and t_m on $\alpha, \beta, \gamma, \delta$, having the matrices

$$R_m=\begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}, \qquad S_m=\begin{pmatrix} a & c & 0 & 0 \\ b & d & 0 & 0 \\ 0 & 0 & a & c \\ 0 & 0 & b & d \end{pmatrix},$$

where R_m is with respect to the units $e_{11}, e_{21}, e_{12}, e_{22}$ of § 8, and S_m is with respect to $e_{11}, e_{12}, e_{21}, e_{22}$. By inspec-

tion A is equivalent to the algebra with the elements R_m and is reciprocal to that with the elements S_m.

If A does not have a modulus, we employ the associative algebra A^* over F with the set of basal units $u_0, u_1, \ldots, u_n$, where the annexed unit u_0 is such that

$$(10)\quad u_0^2=u_0, \qquad u_0u_i=u_i=u_iu_0 \qquad (i=1, \ldots, n),$$

and hence is the modulus of A^*. Write

$$(11)\quad x^*=\xi_0u_0+x, \qquad z^*=\zeta_0u_0+z, \qquad z^{*\prime}=\zeta_0'u_0+z',$$

where x, z, z' are the elements of A displayed above (3). Then

$$x^*z^{*\prime}=\xi_0\zeta_0'u_0+x\zeta_0'+\xi_0z'+xz'.$$

Equating this to z^*, we obtain the transformation

$$(12)\quad \begin{cases} \zeta_0=\xi_0\zeta_0', \qquad \zeta_k=\xi_k\zeta_0'+\xi_0\zeta_k'+\sum_{i,j}\xi_i\gamma_{ijk}\zeta_j' \\ \qquad\qquad (k=1, \ldots, n). \end{cases}$$

The matrix of the coefficients of $\zeta_0', \zeta_1', \ldots, \zeta_n'$ is $R_{x^*}^*$. The latter are the elements of an algebra equivalent to A^* by Theorem 2. Now x^* is in A if $\xi_0=0$. Hence the elements x of A are in one-to-one correspondence with the matrices

$$(13)\quad R_x^*=\begin{pmatrix} 0 & 0 & \ldots & 0 \\ \xi_1 & \rho_{11} & \ldots & \rho_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ \xi_n & \rho_{n1} & \ldots & \rho_{nn} \end{pmatrix}$$

Note that (13) is obtained by bordering matrix R_x in (6) with a front column of ξ's and then a top row of zeros. Write $x'=\Sigma\xi_j'u_j$. Then

$$xx'=\Sigma p_k u_k\,, \qquad p_k=\sum_j \rho_{kj}\xi_j'\,.$$

We verify at once that the product $R_x^*R_{x'}^*$ is $R_{xx'}^*$ since it is obtained by bordering matrix $R_{xx'}=R_xR_{x'}$ with a front column of p's and a top row of zeros. Again, (9) imply the corresponding equations in R^*.

THEOREM 3. *Any associative algebra A (without a modulus) is equivalent to the algebra whose elements are the bordered first matrices* (13) *of the elements x of A, and is reciprocal to the algebra whose elements are the bordered second matrices S_x^* of the elements x of A.*

Here S_x^* is obtained by bordering matrix S_x with a front column of ξ's and a top row of zeros, and hence may be derived from (13) by replacing each ρ_{kj} by σ_{kj}.

THEOREM 4. *Every transformation T_x is commutative with every transformation t_y. Hence*

$$R_xS_y=S_yR_x \tag{14}$$

for all elements x and y of A if and only if A is associative.

For, if we apply first transformation $z=xz'$ and afterward transformation $z'=z''y$, we obtain

$$T_xt_y: \qquad z=x\cdot z''y\,.$$

But if we apply first $t_y: z=z'y$ and afterward $T_x: z'=xz''$, we get

$$t_yT_x: \qquad z=xz''\cdot y\,.$$

The group of the transformations T_x and the group of t_y are said to be a pair of *reciprocal groups* in Lie's

theory of continuous groups. This was the origin of the term "reciprocal algebras" (§ 12).

59. Characteristic determinant and equation of a matrix. Let x be an n-rowed square matrix with elements in a field F. Let ω be an indeterminate. Write

$$f(\omega)=|x-\omega I| \tag{15}$$

for the determinant of matrix $x-\omega I$. Thus $f(\omega)$ is a polynomial of degree n in ω with coefficients in F. It was proved at the end of § 3 that

$$(x-\omega I)\text{adj.}\,(x-\omega I)\equiv f(\omega)I. \tag{16}$$

Each member may be expressed as a polynomial **in** ω whose coefficients are matrices independent of ω. Hence the coefficients of like powers of ω are equal. Thus, if m is any matrix commutative with x, the corresponding polynomials obtained by replacing ω by m are identical, and the same is true of the members of (16). But if we take $m=x$ and replace ω by x in the left member of (16), we obtain the matrix 0. Hence $f(x)I=0$.

We shall call $f(\omega)$ and $f(\omega)=0$ the *characteristic determinant* and *characteristic equation* of matrix x.

THEOREM. *Any matrix x is a root of its characteristic equation. It is understood that when ω is replaced by x the constant term c of $f(\omega)$ is replaced by cI.*

60. Characteristic matrices, determinants, and equations of an element of an algebra. Let $g(\omega)$ be any polynomial with coefficients in F which has a constant term $c\neq 0$ only when the associative algebra A over F has a modulus e and then the corresponding polynomial $g(x)$ in the element x of A has the term ce. Then *the first and second matrices of $g(x)$ are*

$$R_{g(x)}=g(R_x), \qquad S_{g(x)}=g(S_x). \tag{17}$$

For, if k is any positive integer, (8) imply

$$R_{x^k}=R_x^k, \qquad S_{x^k}=S_x^k.$$

Multiply each member by the coefficient of ω^k in $g(\omega)$, sum as to k, and apply (9) and the similar equations in S. We get (17).

First, let A have a modulus. Choose in turn as $g(x)$ the characteristic determinants $\delta(\omega)$ and $\delta'(\omega)$ of matrices R_x and S_x, respectively. Then, by (17) and § 59,

$$R_{\delta(x)}=\delta(R_x)=0, \qquad S_{\delta'(x)}=\delta'(S_x)=0.$$

Hence $\delta(x)=0$, $\delta'(x)=0$ by Theorem 1 of § 58.

Second, let A lack a modulus and extend it to an algebra A^* with a modulus u_0 defined by (10). Choose in turn as $g(x)$ the characteristic determinants of matrices R_x^* and S_x^*, which by (13) are evidently equal to $-\omega\delta(\omega)$ and $-\omega\delta'(\omega)$, respectively. By the facts used in the proof of Theorem 3 of § 58, equations (17) hold when R and S are replaced by R^* and S^*, respectively. Hence (§ 59),

$$R^*_{-x\delta(x)}=0, \qquad S^*_{-x\delta'(x)}=0.$$

Since A^* has a modulus, Theorem 1 of § 58 shows that the subscripts are zero.

THEOREM.* *For every element x of any associative algebra A, $x\delta(x)=0$, $x\delta'(x)=0$. If A has a modulus, also $\delta(x)=0$, $\delta'(x)=0$.*

* For another proof, with an extension to any non-associative algebra, see the author's *Linear Algebras* (Cambridge, 1914), pp. 16–19. That proof is based on the useful fact that if we express xu_j as a linear function of $u_1, \ldots, u_n$ and transpose, we obtain n linear homogeneous equations in $u_1, \ldots, u_n$ the determinant of whose coefficients is $\delta(x)$. Similarly, starting with u_jx we obtain $\delta'(x)$. Compare § 95.

Let x be an element of any algebra A which need not be associative nor have a modulus. The matrices

$$R_x-\omega I=(\rho_{kj}-\omega\delta_{kj}), \qquad S_x-\omega I=(\sigma_{kj}-\omega\delta_{kj}),$$

in which $\delta_{jj}=1$, $\delta_{kj}=0 (k\neq j)$, are called the *first* and *second characteristic matrices* of x, while their determinants $\delta(\omega)$ and $\delta'(\omega)$ are called the *first* and *second characteristic determinants* of x. Thus the first characteristic matrix of x is obtained by subtracting ω from each diagonal element of the first matrix R_x of x.

When A is associative, $\delta(\omega)=0$ or $\omega\delta(\omega)=0$ and $\delta'(\omega)=0$ or $\omega\delta'(\omega)=0$ are called the *first* and *second characteristic equations* of x, according as A has or lacks a modulus.

These terms are all relative to the chosen set of basal units $u_1, \ldots, u_n$ of A. However, we shall next prove that $\delta(\omega)$ and $\delta'(\omega)$ are independent of the choice of the units.

61. Transformation of units. This concept was introduced in § 6. But we now need explicit formulae.

Let $u_1, \ldots, u_n$ be a set of basal units of any algebra A, not necessarily associative, over a field F. We may introduce as new units any n linearly independent elements of A:

$$u_i'=\sum_{j=1}^{n}\tau_{ij}u_j \qquad (i=1, \ldots, n), \tag{18}$$

where the τ_{ij} are numbers of F of determinant $|\tau_{ij}|\neq 0$. Then equations (18) are solvable for the u_j; let the solution be

$$(19) \qquad u_t = \sum_{i=1}^{n} \lambda_{ti} u_i' \qquad (t = 1, \ldots, n),$$

where the λ_{ti} are numbers of F. Elimination of the u_i' between (18) and (19) gives

$$(20) \qquad \sum_{i=1}^{n} \lambda_{ti}\tau_{ij} = \begin{cases} 0 \text{ if } t \neq j \\ 1 \text{ if } t = j \end{cases} \qquad (t, j = 1, \ldots, n).$$

By means of (19), any element $x = \Sigma \xi_t u_t$ of A can be expressed in terms of the new units u_i' as follows:

$$(21) \qquad x = \sum_{t,\, i=1}^{n} \xi_t \lambda_{ti} u_i' = \sum_{i=1}^{n} \xi_i' u_i', \qquad \xi_i' = \sum_{t=1}^{n} \lambda_{ti} \xi_t .$$

By (18) and (1),

$$u_i' u_j' = \sum_{r,\, s=1}^{n} \tau_{ir}\tau_{js} u_r u_s = \sum_{r,\, s,\, h=1}^{n} \tau_{ir}\tau_{js}\gamma_{rsh} u_h .$$

Replacing u_h by its expression from (19), we get

$$(22) \qquad u_i' u_j' = \sum_{k=1}^{n} \gamma_{ijk}' u_k', \qquad \gamma_{ijk}' = \sum_{r,\, s,\, h=1}^{n} \tau_{ir}\tau_{js}\gamma_{rsh}\lambda_{hk},$$

which gives the multiplication table of the new units.

62. Characteristic determinants are invariants. Let R_x' and S_x' be the first and second matrices of x with respect to the new units $u_1', \ldots, u_n'$ defined by (18). We seek the sum analogous to (6), but written in the accented letters ξ', γ' defined by (21) and (22):

$$\rho_{kj}' = \sum_{i=1}^{n} \xi_i' \gamma_{ijk}' = \Sigma \lambda_{ti}\tau_{ir}\tau_{js}\gamma_{rsh}\lambda_{hk}\xi_t ,$$

summed for $i, t, r, s, h = 1, \ldots, n$. Applying first (20) and afterward (6), we get

$$\rho'_{kj} = \sum_{r,s,h} \tau_{js}\gamma_{rsh}\lambda_{hk}\xi_r = \sum_{s,h} \tau_{js}\rho_{hs}\lambda_{hk}\,.$$

Write l_{kh} for λ_{hk}, and t_{sj} for τ_{js}. Let T be the matrix having t_{sj} as the element in the sth row and jth column. By (20), $\Sigma t_{ji}l_{it} = 0$ or 1 according as $j \neq t$ or $j = t$. Hence T^{-1} is the matrix having l_{it} as the element in the ith row and tth column. Then $\rho'_{kj} = \Sigma l_{kh}\rho_{hs}t_{sj}$ gives

$$R'_x = T^{-1}R_xT\,, \qquad S'_x = T^{-1}S_xT\,,$$

the second being derived similarly by using (7) instead of (6). Thus, if ω is an indeterminate,

$$R'_x - \omega I = T^{-1}(R_x - \omega I)T\,, \qquad S'_x - \omega I = T^{-1}(S_x - \omega I)T\,.$$

Passing to determinants, we get

$$|R'_x - \omega I| = |R_x - \omega I|\,, \qquad |S'_x - \omega I| = |S_x - \omega I|\,.$$

THEOREM. *Each characteristic determinant of an element x of an algebra, not necessarily associative, over a field F, is invariant under every linear transformation of units with coefficients in F. The same is therefore true of their constant terms $\Delta(x)$ and $\Delta'(x)$.*

63. Lemma on matrices. *If $a_1, \ldots, a_n$ are the roots of the characteristic equation $f(\omega) = 0$ of an n-rowed square matrix m whose elements belong to a field F, and if $g(\omega)$ is any polynomial with coefficients in F, then the roots of the characteristic equation of the matrix* $g(m)$ are $g(a_1), \ldots, g(a_n)$.*

* With the term cI if the constant term of $g(\omega)$ is c.

By chapter xi, we may extend F to a field F' in which $f(\omega)\cdot g(\omega)$ decomposes into linear functions of ω:

$$f(\omega)=(\alpha_1-\omega)\ldots.(\alpha_n-\omega), \qquad g(\omega)=\beta(\omega-\beta_1)\ldots.(\omega-\beta_r)$$

If I is the n-rowed unit matrix, we have in F'

$$g(m)=\beta(m-\beta_1 I)\ldots.(m-\beta_r I).$$

Passing to determinants, we get

$$|g(m)|=\beta^n|m-\beta_1 I|\ldots.|m-\beta_r I|=\beta^n f(\beta_1)\ldots.f(\beta_r).$$

But, by the initial formulae,

$$f(\beta_j)=(\alpha_1-\beta_j)\ldots.(\alpha_n-\beta_j),$$
$$g(\alpha_k)=\beta(\alpha_k-\beta_1)\ldots.(\alpha_k-\beta_r).$$

Hence

$$|g(m)|=g(\alpha_1)\ldots.g(\alpha_n). \tag{23}$$

Let ξ be a variable in the field F' and write $h(\omega, \xi)$ for $g(\omega)-\xi$. Then $h(m, \xi)=g(m)-\xi I$, so that the characteristic determinant of $g(m)$ is the determinant of $h(m, \xi)$. Applying (23) with the polynomial $g(m)$ replaced by $h(m, \xi)$, we see that the determinant of the latter is equal to the product

$$h(\alpha_1, \xi)\ldots.h(\alpha_n, \xi)=[g(\alpha_1)-\xi]\ldots.[g(\alpha_n)-\xi].$$

Equating the latter to zero, we therefore obtain the characteristic equation of matrix $g(m)$. Hence its roots are $g(\alpha_1), \ldots., g(\alpha_n)$.

64. Roots of the characteristic equation of $g(x)$.

THEOREM. *Let $g(\omega)$ be a polynomial of the type in* § 60. *Let F_1 be an extension of the field F such that the first (or second) characteristic equation of the element x of*

the algebra is solvable in F_1 and has the roots $a_1, \ldots, a_n$. Then the roots of the first (or second) characteristic equation of $g(x)$ are $g(a_1), \ldots, g(a_n)$.

For, the first characteristic equation of x is $|R_x - \omega I| = 0$, which is the characteristic equation of matrix R_x, and has the roots $a_1, \ldots, a_n$. Hence by § 63 with $m = R_x$, the roots of the characteristic equation of matrix $g(R_x)$ are $g(a_1), \ldots, g(a_n)$. By (17_1) they are the roots of

$$|R_{g(x)} - \omega I| = 0,$$

which is the first characteristic equation of $g(x)$.

COROLLARY*. *An element x is nilpotent if and only if every root of either characteristic equation of x is zero.*

For, if $x^r = 0$ and if there be a root $\rho \neq 0$, the corresponding characteristic equation of x^r would have the root $\rho^r \neq 0$, whereas either characteristic equation of the element 0 is evidently $\omega^n = 0$.

Conversely, if every root of either characteristic equation is zero, that equation is evidently $\omega^n = 0$, and by the theorem in § 60 x is a root of the latter or of its product by ω.

65. Traces, properly nilpotent elements. The sum of the diagonal elements of the first matrix R_x of x is called the *(first) trace* of x, and is denoted by t_x.

The first characteristic equation of x is

$$|R_x - \omega I| \equiv (-1)^n [\omega^n - t_x \omega^{n-1} + \ldots] = 0.$$

Hence t_x is equal to the sum of the roots, and (§ 62) is independent of the choice of the basal units of the algebra.

* This follows at once from the theorem in § 68.

In the proof of the next theorem it will be seen that we must exclude fields F having a *modulus* p, i.e., an integer p such that $px=0$ for every x in F. When p is a prime, one such field is composed of the classes of residues of integers modulo p, as explained in detail in § 110. Any sub-field of the field of all complex numbers has no modulus.

THEOREM. *An element x of an associative algebra A over a non-modular field F is zero or properly nilpotent if and only if $t_{xy}=0$ for every y in A.*

First, let x be zero or properly nilpotent, so that xy is nilpotent. Then all the roots of the first characteristic equation of xy are zero by the corollary in § 64, whence their sum t_{xy} is zero.

Conversely, let $t_{xy}=0$ for every y in A. Since

$$(xy)^r=xy_1, \qquad y_1=(yx)^{r-1}y,$$

$t_z=0$, where $z=(xy)^r$, for every positive integer r. In the theorem of § 64 take $g(\omega)\equiv\omega^r$ and replace x by xy; hence the roots of the first characteristic equation of $z=(xy)^r$ are the rth powers of the roots of that of xy. The sum t_z of the former roots was seen to be zero. Hence the sum s_r of the rth powers of the roots of the first characteristic equation

$$f(\omega)\equiv\omega^n+\gamma_1\omega^{n-1}+\ \ldots\ .\ +\gamma_n=0$$

of xy is zero for every positive integer r. For any field F, we have Newton's identities,

$$s_j+\gamma_1 s_{j-1}+\gamma_2 s_{j-2}+\ \ldots\ .\ +\gamma_{j-1}s_1+j\gamma_j=0 \qquad (j=1,\ \ldots\ .\ ,\ n).$$

Since each $s_r = 0$, we have $j\gamma_j = 0$. Hence $\gamma_j = 0$, since F has no modulus. Thus $f(\omega) \equiv \omega^n = 0$. Since every root of this characteristic equation of xy is zero, the corollary in § 64 shows that xy is nilpotent for every y, whence x is zero or properly nilpotent.

But if F has a modulus the prime n, γ_n need not be zero, although $\gamma_j = 0 (j < n)$. Take $\gamma_n = -1$. Then

$$f(\omega) = \omega^n - 1 \equiv (\omega - 1)^n \pmod{n},$$

so that all the roots are 1 and $s_r \equiv 0 \pmod{n}$ for every r.

To show that not merely our proof, but also the theorem itself, may fail for a modular field, take $n = 2$ in what precedes and consider the algebra $(1, e)$ where $e^2 = 0$, over the field of classes of residues of integers modulo 2. The first matrix of $x = \xi + \eta e$ has the diagonal elements ξ, ξ. Hence the trace of every x is $2\xi \equiv 0 \pmod{2}$. The elements 1 and $1 + e$ are not nilpotent, although the traces of their products by every y were seen to be zero.

66. To make an important application of the preceding theorem, consider

$$x = \sum_i \xi_i u_i, \qquad y = \sum_j \eta_j u_j, \qquad xy = \sum_{i,j} \xi_i \eta_j u_i u_j.$$

Relations (9) evidently imply

$$t_{ax} = a t_x, \qquad t_{x+y} = t_x + t_y. \tag{24}$$

Hence if the trace of $u_i u_j$ is τ_{ij},

$$t_{xy} = \sum_{i,j=1}^{n} \tau_{ij} \xi_i \eta_j. \tag{25}$$

This is zero for every y in A if and only if

$$\sum_{i=1}^{n} \tau_{ij}\xi_i = 0 \qquad (j = 1, \ldots, n). \tag{26}$$

Hence $x = \Sigma \xi_i u_i \neq 0$ is properly nilpotent in A if and only if relations (26) hold (with $\xi_1, \ldots, \xi_n$ not all zero).

THEOREM. *Let the n-rowed square matrix* (τ_{ij}), *in which* τ_{ij} *is the trace of* $u_i u_j$, *be of rank* r. An algebra A over a non-modular field has no properly nilpotent elements (and hence is semi-simple) if and only if* $r = n$. *Also, A has a maximal nilpotent invariant sub-algebra N of order* ν *if and only if* $\nu = n - r > 0$. *The value of r depends solely upon the constants of multiplication of A.*

The reader is now in a position to follow the proof in chapter viii of the principal theorem on algebras.

For an important application to the arithmetic of algebras, we shall need the explicit expression for τ_{sj}, which is the trace of $u_s u_j = \Sigma \gamma_{sji} u_i$ and hence is the sum of the diagonal elements of the first matrix of the element obtained from $x = \Sigma \xi_i u_i$ by replacing ξ_i by γ_{sji}. A diagonal element of the first matrix of x is given by (6) with $j = k$. Hence

$$\tau_{sj} = \sum_{i,k=1}^{n} \gamma_{sji}\gamma_{ikk}. \tag{27}$$

* A matrix is said to be of *rank r* if at least one r-rowed minor is not zero, while every $(r+1)$-rowed minor is zero. Then r of the ξ_i in (26) are expressible uniquely in terms of the remaining $n-r$, which are arbitrary. See Dickson's *First Course in the Theory of Equations* (1922), p. 116.

67. Minimum equation of a matrix. Any square matrix m with elements in a field F is a root of its characteristic equation (§ 59) and hence is a root of a unique equation $\phi(\omega)=0$ of lowest degree whose coefficients belong to F, the leading coefficient being unity. This equation is called the *minimum* (or reduced) equation of m. It is understood that when ω is replaced by m, the constant term of $\phi(\omega)$ is multiplied by the unit matrix I.

LEMMA. *If* $\lambda(m)=0$, *where* $\lambda(\omega)$ *is a polynomial with coefficients in* F, *then* $\lambda(\omega)$ *is exactly divisible by* $\phi(\omega)$.

For, let $q(\omega)$ and $r(\omega)$ denote the quotient and remainder from the division of $\lambda(\omega)$ by $\phi(\omega)$, where $r(\omega)$ is either zero identically or is of degree less than that of $\phi(\omega)$. Then

$$\lambda(\omega)\equiv q(\omega)\phi(\omega)+r(\omega).$$

Hence $r(m)=0$, so that $r(\omega)$ is zero identically.

THEOREM 1. *The minimum equation of an* n*-rowed square matrix* m *is* $q(\omega)=0$, *where* $q(\omega)$ *is the quotient of the characteristic determinant* $f(\omega)$ *of* m *by the greatest common divisor* $g(\omega)$ *of its* $(n-1)$*-rowed minors.*

Denote the adjoint matrix (§ 3) of $m-\omega I$ by $(m-\omega I)_0$. Each of its elements is divisible by $g(\omega)$. Hence

$$(m-\omega I)_0\equiv g(\omega)M,$$

where M is a matrix whose elements are polynomials in ω without a common factor other than a number of F. Hence (16) with $x=m$ becomes

$$g(\omega)M(m-\omega I)\equiv f(\omega)I\equiv g(\omega)q(\omega)I.$$

We may delete the common factor $g(\omega)$ from this identity in matrices since it is equivalent to n^2 equations between elements of the n-rowed matrices. Thus

$$M(m-\omega I)\equiv q(\omega)I\,. \tag{28}$$

As in § 59 this identity holds true after ω is replaced by any matrix commutative with m, say m itself. Hence $q(m)=0$. By the lemma, $q(\omega)$ is divisible by $\phi(\omega)$.

If ρ is another indeterminate, we have

$$\phi(\omega)-\phi(\rho)\equiv\psi(\omega,\,\rho)(\rho-\omega)\,,$$

where $\psi(\omega,\,\rho)$ is a polynomial in ω and ρ with coefficients in F. We may replace ρ by m and, since $\phi(m)=0$, obtain

$$\phi(\omega)I\equiv\psi(\omega,\,m)(m-\omega I)\,.$$

From this and (28), we deduce

$$q(\omega)\psi(\omega,\,m)(m-\omega I)\equiv\phi(\omega)M(m-\omega I)\,.$$

We may delete the common factor $m-\omega I$ whose determinant is not zero identically in ω. Since the elements of M have no common factor, $q(\omega)$ must divide $\phi(\omega)$.

Our two results show that $q(\omega)$ and $\phi(\omega)$ differ only by a factor belonging to the field F. Hence the theorem is proved.

THEOREM 2. *Every root of the characteristic equation $f(\omega)=0$ of a matrix is a root of its minimum equation $\phi(\omega)=0$, and conversely.*

For, if we pass from (28) to determinants, we have

$$|M|\cdot f(\omega)\equiv[\phi(\omega)]^n\,.$$

The converse is true by Theorem 1.

68. Minimum equation of an element of an algebra. Let x be an element of an associative algebra A over F. If A has a modulus, any polynomial $g(\omega)$ with coefficients in F which vanishes when $\omega = R_x$ vanishes for $\omega = x$ by (17) and Theorem 1 of § 58, and conversely. Hence the minimum equation of R_x is the minimum equation of x. By the preceding Theorem 2, every root of the former is a root of the characteristic equation of R_x, which is the first characteristic equation $\delta(\omega) = 0$ of x by § 60, and conversely. The same holds for S_x and $\delta'(\omega) = 0$. If A lacks a modulus, we employ R_x^* instead of R_x and note (§ 60) that (17) still hold.

THEOREM. *Every root of the minimum equation of an element x of any associative algebra is a root of either characteristic equation of x and conversely.*

69. Rank equation. By § 11 the quaternion

$$q = \sigma + \xi i + \eta j + \zeta k,$$

in which σ, ξ, η, ζ are independent real variables, is a root of

$$\omega^2 - 2\sigma\omega + (\sigma^2 + \xi^2 + \eta^2 + \zeta^2) = 0,$$

and is evidently not a root of an equation of the first degree. This quadratic equation is called the *rank equation* of the *general* real quaternion q since its coefficients are polynomials in σ, ξ, η, ζ and the coefficient of ω^2 is unity, and since q is not the root of an equation of lower degree whose coefficients have these properties.

Consider any associative algebra A over a field F. Let $u_1, \ldots, u_n$ be a set of basal units of A. Let $\xi_1, \ldots, \xi_n$ be variables ranging independently over F. By § 60, the element $x = \Sigma \xi_i u_i$ of A is a root of $\omega\delta(\omega) = 0$,

where $\delta(\omega)$ is the first characteristic determinant of x and is a polynomial in ω whose coefficients are polynomials in $\xi_1, \ldots, \xi_n$ with coefficients in F.

Hence there exists a least positive integer r such that x is a root of an equation of degree r,

$$c_0\omega^r + c_1\omega^{r-1} + \ldots = 0, \tag{29}$$

with or without a constant term according as A has or lacks a modulus, where each c_i is a polynomial in $\xi_1, \ldots, \xi_n$ with coefficients in F, while c_0 is not zero identically.

When $\xi_1, \ldots, \xi_n$ are indeterminates, $c_0, c_1, \ldots$ have a greatest common divisor g by Theorem V of § 114. Write $c_i = gq_i$. Then (29) becomes $gR(\omega) = 0$, where

$$R(\omega) = q_0\omega^r + q_1\omega^{r-1} + \ldots \tag{30}$$

Here $q_0, q_1, \ldots$ have no common divisor other than a number of F, and q_0 is not zero identically. These properties remain true when we interpret $\xi_1, \ldots, \xi_n$ as independent variables of F, provided F be an infinite field as we shall assume henceforth.*

By means of $x = \Sigma\xi_i u_i$ and the multiplication table (1) of the units u_i, we may express $R(x)$ in the form $\Sigma f_i u_i$, where f_i is a polynomial in $\xi_1, \ldots, \xi_n$ with coefficients in F. Since $gR(x) = 0$, each $gf_i = 0$. By III of § 112, the corresponding function gf_i of indeterminates $\xi_1, \ldots, \xi_n$ is zero identically, so that one factor is

* For, if f, g, h are polynomials in $\xi_1, \ldots, \xi_n$ with coefficients in F, and if $f = gh$ when the ξ's are indeterminates, evidently $f = gh$ when the ξ's are independent variables in F. What we need is the converse, and it is true by III of § 112.

zero by the theorem in § 111. Since g is not zero identically, each $f_i \equiv 0$ and $R(x) = 0$.

LEMMA. *If* $\lambda(x) = 0$, *where* $\lambda(\omega)$ *is a polynomial in* ω *whose coefficients are polynomials in* $\xi_1, \ldots, \xi_n$ *with coefficients in* F, *then* $\lambda(\omega)$ *is exactly divisible by* $R(\omega)$ *when* $\xi_1, \ldots, \xi_n$ *are indeterminates.*

For, let $g(\omega)$ denote the greatest common divisor of $\lambda(\omega)$ and $R(\omega)$. By V of § 114, there exist polynomials $s(\omega)$ and $t(\omega)$ whose coefficients are polynomials in $\xi_1, \ldots, \xi_n$ with coefficients in F and a polynomial p in $\xi_1, \ldots, \xi_n$ with coefficients in F such that

$$s(\omega)\lambda(\omega) + t(\omega)R(\omega) \equiv pg(\omega).$$

Hence $pg(x) = 0$. By the paragraph preceding the lemma, $g(x) = 0$. Hence the degree of $g(\omega)$ in ω is not less than the degree of $R(\omega)$ in view of the definition of the latter. But the degree of the divisor $g(\omega)$ is not greater than that of the dividend $R(\omega)$. Hence the degrees are equal. Then by IV of § 114 with $\rho = 1$, $K = 1$, $R(\omega)$ is the product of $g(\omega)$ by an element of F. Since $\lambda(\omega)$ is divisible by $g(\omega)$, it is divisible by $R(\omega)$.

As noted above, $\omega\delta(\omega)$ is a polynomial having the properties assumed for $\lambda(\omega)$ in the lemma, and hence is divisible by $R(\omega)$. Since the coefficient of the highest power of ω in $\omega\delta(\omega)$ is ± 1, we conclude that that of $R(\omega)$ is a divisor of ± 1. Hence q_0 is a number of F and may be made equal to unity by dividing the terms of $R(\omega)$ by it.

THEOREM. *Let* A *be any associative algebra over an infinite field* F. *If* $\xi_1, \ldots, \xi_n$ *are independent variables of* F, *the element* $x = \Sigma \xi_i u_i$ *is a root of a uniquely*

determined **rank equation** $R(\omega)=0$ *in which the coefficient of the highest power* ω^r *is unity, while the remaining coefficients are polynomials in* $\xi_1, \ldots, \xi_n$ *with coefficients in* F. *Also,* x *is not a root of any equation of degree* $<r$ *all of whose coefficients are such polynomials.*

The integer r is called the *rank* of algebra A.

COROLLARY. *If* A *has a modulus* e, *the constant term* c *of* $R(\omega)$ *is not zero identically.*

For, $R(\omega)$ divides $\delta(\omega)$, so that c divides $\delta(0)=\Delta(x)$. But $\Delta(e)=1$ by the footnote in § 58.

The theorem fails for finite fields. Consider the algebra $A=(u_1, u_2, u_3)$ over the field composed of the two classes of residues of integers modulo 2, where $u_i^2=u_i$, $u_iu_j=0 (j\neq i)$. The modulus of A is $e=\Sigma u_i$. Either characteristic determinant is

$$\Delta=(\xi_1-\omega)(\xi_2-\omega)(\xi_3-\omega).$$

Evidently every element x of A is a root of $\omega^2=\omega$. Now

$$\Delta\equiv(\omega-\omega^2)(\omega+1+\xi_1+\xi_2+\xi_3)+\rho \pmod 2,$$

where

$$\rho=s\omega-\xi_1\xi_2\xi_3, \qquad s=1+\Sigma\xi_1+\Sigma\xi_1\xi_2.$$

Thus $sx-\xi_1\xi_2\xi_3e=0$ for every x in A. Another such linear equation satisfied by x is $\sigma x=0$ where $\sigma=(1-\xi_1)(1-\xi_2)(1-\xi_3)$.

70. Let x be an element of A whose co-ordinates $\xi_1, \ldots, \xi_n$ are independent variables in F. As in § 68, the rank equation $R(\omega)=0$ of x is the minimum equation of matrices R_x and S_x (or of R_x^* and S_x^* if A has no modulus). The discussion* in § 67 is seen to hold

* An indirect proof of the lemma consists in seeing that it is a translation of that in § 69.

when m is interpreted as one of the preceding four matrices, say R_x, since the leading coefficient of $\phi(\omega) \equiv R(\omega)$ is unity, while the remaining coefficients are now polynomials in $\xi_1, \ldots, \xi_n$ with coefficients in F.

THEOREM. *The distinct factors irreducible in an infinite field F of the left member of either characteristic equation of x coincide with the distinct irreducible factors of the rank function $R(\omega)$.*

71. Rank equation of a simple matric algebra. By § 59, any n-rowed square matrix $x = (x_{ij})$ with elements in F is a root of

$$(31) \quad R(\omega) \equiv (-1)^n \, | \, x_{ij} - \delta_{ij}\omega \, | \, = 0, \quad \delta_{ii} = 1, \quad \delta_{ij} = 0 (i \neq j).$$

Let the x_{ij} be n^2 independent variables of an infinite field F. We shall prove that $R(\omega) = 0$ is the rank equation. This will follow from the lemma in § 69 if we prove that $R(\omega)$ is irreducible in F. It suffices to prove that its constant term $\pm |x_{ij}|$ is irreducible in F. In view of the footnote in § 69, this follows from the

LEMMA. *The determinant $|x_{ij}|$ of n^2 indeterminates $x_{ij} (i, j = 1, \ldots, n)$ is a polynomial $f(x_{11}, x_{12}, \ldots, x_{nn})$ which is irreducible in every field F.*

Suppose that f is a product of two polynomials g and h with coefficients in F. Since f is of degree 1 in each indeterminate, we may assume that g is of degree 0 and h of degree 1 in x_{11}. No term of the expansion f of $|x_{ij}|$ contains the product of x_{11} by an element x_{r1} of the first column. Hence g is of degree 0 in x_{r1}, since otherwise $x_{r1}x_{11}$ would occur in a term of $gh = f$. Thus h is of degree 1 in x_{r1}. Since $x_{rc}x_{r1}$ does not occur in a term of $gh = f$, g is of degree 0 in every x_{rc}.

THEOREM. *The rank equation of the algebra of all n-rowed square matrices* (x_{ij}) *with elements in any infinite field is its characteristic equation* (31).

Hence by § 70 the characteristic determinant of x is the nth power of $R(\omega)$ apart from sign.

72. Rank equation of a direct sum. *If an associative algebra A with the modulus* e over an infinite† field F is a direct sum of algebras* $A_1, \ldots, A_t$, *and if* $R(\omega)=0$ *is the rank equation of A, and* $R_i(\omega)=0$ *is that of* A_i, *then* $R(\omega)\equiv R_1(\omega) \ldots R_t(\omega)$.

The co-ordinates ξ_{ij} $(j=1, \ldots, n_i)$ of the general element x_i of A_i are independent variables in F. The general element $x=\Sigma x_i$ of A has as co-ordinates the independent variables ξ_{ij} $(j=1, \ldots, n_i;\ i=1, \ldots, t)$ in F. If also $y=\Sigma y_i$, then $xy=\Sigma x_i y_i$, whence

$$x^k=\Sigma x_i^k, \qquad 0=R(x)=\Sigma R(x_i).$$

Hence each $R(x_i)=0$. By the lemma and the footnote in § 69, $R(\omega)$ is divisible by the $R_i(\omega)$ and hence by their least common multiple $L(\omega)$ when the ξ_{ij} are indeterminates. Write $L(\omega)\equiv R_i(\omega)Q_i(\omega)$. Then $L(x_i)=0$, whence $L(x)=\Sigma L(x_i)=0$, so that $L(\omega)$ is divisible by $R(\omega)$ by the same lemma. The two results show that $R(\omega)$ is the least common multiple of the $R_i(\omega)$.

The theorem will therefore follow if we prove that no two of the $R_i(\omega)$ have a common divisor of degree >0. Suppose that $R_1(\omega)$ and $R_2(\omega)$ have a common divisor $D(\omega)$ of degree >0. Since $R_1(\omega)$ is of degree 0 in the

* The theorem may fail if there is no modulus since the rank equation of a zero algebra is always $\omega^2=0$.

† The theorem fails for the algebra $(u_1)\oplus(u_2)\oplus(u_3)$, $u_i^2=u_i$ over the field of order 2, since its rank equation is linear (end of § 69), while that of (u_i) is $\omega-\xi_i=0$.

ξ_{2j}, and $R_2(\omega)$ is of degree 0 in the ξ_{1j}, $D(\omega)$ is of degree 0 in both sets and hence involves the single indeterminate ω. But

$$R_1(\omega)=\omega^{r_1}+c_1\omega^{r_1-1}+\ \ldots\ ,$$

where $c_1, \ldots$ are homogeneous polynomials in the ξ_{1j} and hence vanish when each $\xi_{1j}=0$. Hence $D(\omega)$ is a divisor ω^d of ω^{r_1}. This is impossible since A_1 has a modulus and hence $R_1(\omega)$ has a constant term not zero identically by the corollary in § 69.

73. Rank equation unaltered by any transformation of units. For an associative algebra A with the constants of multiplication γ_{ijk}, let $R(\omega;\ \xi_i,\ \gamma_{ijk})=0$ be the rank equation which is satisfied by $\omega=x$, where $x=\Sigma\xi_i u_i$ is the general element of A. Under a transformation of units (§ 61), let x become $x'=\Sigma\xi_i' u_i'$, and let R become $\rho(\omega;\ \xi_i',\ \gamma_{ijk}')$. For $\omega=x'$, both ρ and $R(\omega;\ \xi_i',\ \gamma_{ijk}')$ are zero; unless they are identical, their difference is zero for $\omega=x'$. Passing back to the initial units, we obtain a function of degree $<r$ which is zero for $\omega=x$, contrary to the definition of r. Hence *the rank equation is independent of the choice of basal units.**

* Another proof follows from the theorems of §§ 62 and 70 and the fact that each irreducible factor of an invariant is an invariant. Compare Bôcher, *Introduction to Higher Algebra* (1907), p. 218.

CHAPTER VIII

THE PRINCIPAL THEOREM ON ALGEBRAS

74. Introduction. We shall prove that any associative algebra over a non-modular field F is either semi-simple or the sum of its maximal nilpotent invariant sub-algebra and a semi-simple algebra, each over F. For the special case in which F is the field of all complex numbers, a more elementary proof is given in § 79.

We shall need to employ extensions of the given field F. In this connection, note that the theorem of § 66 implies the

COROLLARY. *Let A be an algebra over a non-modular field F. Let F_1 denote any field containing F as a sub-field. Denote by A_1 the algebra over F_1 which has the same basal units* (and hence the same constants of multiplication) as algebra A over F. Then A_1 is semi-simple if and only if A is semi-simple. But if A has a maximal nilpotent invariant sub-algebra N, that of A_1 is the algebra over F_1 which has the same basal units as N.*

75. Direct product of simple matric algebras. Let A be a simple matric algebra over F with the m^2 basal units a_{ij} such that (§ 51)

$$(1) \quad a_{ij}a_{rs}=0 \quad (j\neq r), \quad a_{ij}a_{js}=a_{is} \quad (i,j,r,s=1,\ldots,m).$$

Let B be a simple matric algebra over F with n^2 basal units $b_{rs}(r, s=1, \ldots, n)$, satisfying relations of

* They may be assumed to be linearly independent with respect to F_1 by § 13.

type (1), such that each b_{rs} is commutative with every a_{ij} and such that the m^2n^2 products $a_{ij}b_{rs}$ are linearly independent with respect to F.

Then those products are the basal units of the direct product $A \times B$ (§ 50). Take them as the elements of a matrix (e_{pq}) which is exhibited compactly as the compound matrix

$$(2) \qquad \begin{pmatrix} (a_{ij})b_{11} & (a_{ij})b_{12} & \cdots & (a_{ij})b_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ (a_{ij})b_{n1} & (a_{ij})b_{n2} & \cdots & (a_{ij})b_{nn} \end{pmatrix},$$

in which the entries themselves are matrices:

$$(3) \qquad (a_{ij})b_{rs} = \begin{pmatrix} a_{11}b_{rs} & a_{12}b_{rs} & \cdots & a_{1m}b_{rs} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1}b_{rs} & a_{m2}b_{rs} & \cdots & a_{mm}b_{rs} \end{pmatrix}.$$

From our two notations for the same element we have

$$P \equiv a_{ij}b_{rs} = e_{i+m(r-1),\ j+m(s-1)},$$

$$Q \equiv a_{kl}b_{tu} = e_{k+m(t-1),\ l+m(u-1)}.$$

Evidently $PQ = 0$ unless $k = j$, $t = s$, and then

$$PQ = a_{il}b_{ru} = e_{i+m(r-1),\ l+m(u-1)}.$$

But $k = j$, $t = s$ imply $j + m(s-1) = k + m(t-1)$ and conversely, since j and k are positive integers $\leqq m$. Hence the e's satisfy relations of type (1) and are therefore the basal units of a simple matric algebra.

THEOREM. *The direct product of two simple matric algebras of orders m^2 and n^2 is a simple matric algebra of order m^2n^2.*

76. Division algebras as direct sums of simple matric algebras.

THEOREM. *If D is a division algebra over a non-modular field F, there exist a finite number of roots of equations with coefficients in F whose adjunction to F gives a field F_1 such that the algebra D_1 over F_1, which has the same basal units as D, is a direct sum of simple matric algebras over F_1.*

Select any element x of D not the product of the modulus e by a number of F. By § 60, x is a root of either characteristic equation, and hence of a certain equation $\phi(\omega)=0$ of minimum degree $s>1$ having coefficients in F.

Let F' be the field obtained by adjoining to F all the roots $\lambda_1, \ldots, \lambda_s$ of $\phi(\omega)=0$. Let D' be the algebra over F' having the same basal units as D. Then

$$(x-\lambda_1 e) \ldots (x-\lambda_s e)=\phi(x)=0$$

in D'. Since x is not the product of e by a number λ_i of F' (footnote in § 74), no one of the $x-\lambda_i e$ is zero, and yet their product is zero. Hence D' is not a division algebra by Theorem 4 of § 43.

The division algebra D is simple (§ 52). Hence by § 74 D' is semi-simple and (§ 40) is either simple or a direct sum of simple algebras over F'. Each such simple algebra is the direct product of a division algebra D_i by a simple matric algebra, each over F' (§ 51). The order of each D_i is less than that of D'; this is evident for the second case in which D' was a direct sum, and also for the first case in which D' was simple, provided the matric factor is of order >1; but the remaining case $i=1$, $D'=D_1$, is excluded since D' is not a division algebra.

If each D_i is of order 1, our theorem holds for $F_1 = F'$. In the contrary case, we employ an extension F'' of F' such that the algebra over F'', having the same $n_i (n_i > 1)$ basal units as D_i, is not a division algebra. To it we apply the argument just made for D'.

Since the division algebras introduced at any stage are all of orders less than those of the preceding stage, the process terminates, so that we reach a final stage in which the division algebras are all of order 1. Each division algebra of the prior stage is therefore a direct sum of simple matric algebras. Our theorem now follows from that in § 75.

77. Theorem.* *If A is an algebra having a single idempotent element e over a non-modular field F, then A can be expressed in the form $A = B + N$, where B is a division algebra and N is zero or the maximal nilpotent invariant sub-algebra of A.*

The theorem is obvious when A is of order 1, since then $A = A + 0$ and A is a division algebra.

To prove the theorem by induction, assume it for all algebras of type A which are of orders less than the order of A.

We first show that we may take $N^2 = 0$. Let $N^2 \neq 0$ and write

$$(4) \quad A = B' + N, \quad B' \wedge N = 0, \quad N = N_1 + N^2, \quad N_1 \wedge N^2 = 0.$$

Since $AN^2 = AN \cdot N \leqq N \cdot N$ and $N^2 A \leqq N^2$, N^2 is an invariant sub-algebra of A.

The classes† (x) of A modulo N^2 are the elements of $A - N^2$. In particular, the classes (n_1), each uniquely

* In § 79 there is a far simpler proof for the case of algebras A over the field of all complex numbers.

† The notation (x) marks the distinction from classes $[x]$ modulo N.

determined by an element n_1 of N_1, form the maximal nilpotent invariant sub-algebra $(N_1) \equiv N - N^2$ of $A - N^2$. Let (B') denote the set of classes modulo N^2 determined by the elements of B'. Then, by (4),

$$A - N^2 = (B') + (N_1).$$

Since $N^2 \neq 0$, the order of $A - N^2$ is less than that of A and hence, by the hypothesis for the induction, we can choose a division sub-algebra (B'') of $A - N^2$ such that

$$A - N^2 = (B'') + (N_1).$$

Write $C = B' + N_1$. Then, by (4), $A = C + N^2$, $C \wedge N^2 = 0$. Those elements c of C, for which classes (c) modulo N^2 belong to (B''), form a linear set B'' of A. But we saw that, when either (B') or (B'') is added to (N_1), we get $A - N^2$, whence $(B'') \equiv (B')$ modulo (N_1). Hence $B'' \equiv B'$ modulo N, so that $A = B'' + N$ by (4).

We had $(B'')^2 = (B'')$ in $A - N^2$. Hence $B''^2 \equiv B''$ modulo N^2 in A. Since N^2 is invariant in A,

$$(B'' + N^2)^2 \leqq B'' + N^2.$$

Hence $A' \equiv B'' + N^2$ is an algebra. It is a proper sub-algebra of A, since $A' < B'' + N = A$ by $N^2 < N$.

Finally, N^2 is a maximal nilpotent invariant sub-algebra of A'. For, if B'' had a properly nilpotent element, (B'') would contain a properly nilpotent element, whereas it is a division algebra. Hence by the hypothesis for the induction, there exists a division sub-algebra B of A' (and hence of A) such that $A' = B + N^2$. But $A' = B'' + N^2$. Thus $B \equiv B''$ modulo N^2 and hence also modulo N. Hence $A = B'' + N$ implies $A = B + N$.

It remains to prove the theorem when $N^2=0$, a property utilized only at the end of the proof.

By § 38, $D=A-N$ is semi-simple and has a modulus. It has no other idempotent element since A has a single one. Hence by Corollary 1 of § 43, D is a division algebra.

By § 76, we may extend the initial field to a field F_1 such that the algebra D_1 over F_1, which has the same basal units as D, is a direct sum of simple matric algebras. Denote by A_1 and N_1 the algebras over F_1 which have the same basal units as A and N, respectively. By § 74, N_1 is the maximal nilpotent invariant sub-algebra of A_1. Hence $A_1-N_1=D_1$.

By § 54, A_1 contains a sub-algebra C equivalent to A_1-N_1, whence $A_1=C+N_1$, $C\wedge N_1=0$. Let $e_1, \ldots, e_c$ be a set of basal units of C. Since $A-N$ is of order c, the basal units of N (or N_1) together with certain c elements $a_1, \ldots, a_c$ of A form a set of basal units of A (or A_1). Hence we may write

$$e_i=\sum_{j=1}^{c} a_{ij}a_j+n_i \qquad (i=1, \ldots, c), \tag{5}$$

where the n_i are elements of N_1, and the a_{ij} are numbers of F_1 whose determinant is not zero (otherwise, as in § 5, a linear combination of $e_1, \ldots, e_c$ would belong to N_1, contrary to $C\wedge N_1=0$). Solving (5), we get

$$a_i=\sum_{j=1}^{c} \beta_{ij}(e_j-n_j) \qquad (i=1, \ldots, c), \tag{6}$$

where the β_{ij} are in F_1 and their determinant is not zero. Write

$$\omega_i = \sum_{j=1}^{c} \beta_{ij} e_j \qquad (i = 1, \ldots, c). \tag{7}$$

Since the e_j are basal units of algebra C,

$$\omega_i \omega_k = \sum_{t=1}^{c} \gamma_{ikt} \omega_t \qquad (i, k = 1, \ldots, c). \tag{8}$$

We may express (6) in the form

$$a_i = \omega_i + \nu_i \qquad (i = 1, \ldots, c), \tag{9}$$

where ν_i is in N_1. Since N_1 is invariant in A_1,

$$a_i a_k = \omega_i \omega_k + n_{ik},$$

where n_{ik} and n'_{ik} below are in N_1. Hence, by (8) and (9),

$$a_i a_k = \sum_{t=1}^{c} \gamma_{ikt} a_t + n'_{ik}, \qquad n'_{ik} = n_{ik} - \sum_{t=1}^{c} \gamma_{ikt} \nu_t .$$

But the product $a_i a_k$ of two elements of A can be expressed in one and only one way as a linear combination, with coefficients in F, of the basal units of A, which are composed of those of N and $a_1, \ldots, a_c$. Hence the γ_{ikt} are numbers of F.

But F_1 was derived from F by the adjunction of a finite number of roots of equations with coefficients in F. Hence $F_1 = F(\xi_1, \xi_2, \ldots)$, where $1, \xi_1, \xi_2, \ldots$ are linearly independent with respect to F. We may therefore write

$$-\nu_i = \nu_{i0} + \nu_{i1}\xi_1 + \nu_{i2}\xi_2 + \ldots,$$

where the ν_{ij} are in N. Write

$$z_i = a_i + \nu_{i0}, \qquad B = (z_1, z_2, \ldots, z_c),$$

where z_i is in A and B is a linear set of elements of A over F. Hence $A=B+N$. Using also (9), we get

$$\omega_i=z_i+n_i\,, \qquad n_i=-\nu_i-\nu_{i0}=\nu_{i1}\xi_1+\nu_{i2}\xi_2+\ \ldots\ldots$$

Substituting in (8), we get

$$(z_i+n_i)\ (z_k+n_k)=\sum_{l=1}^{c}\gamma_{ikl}(z_l+n_l)\,.$$

Since $n_in_k=0$ by $N_1^2=0$, the left member is the sum of z_iz_k (which is in A and hence is free of $\xi_1, \xi_2, \ldots$) and the linear homogeneous function $z_in_k+n_iz_k$ of $\xi_1, \xi_2, \ldots\ldots$ Equating the parts free of $\xi_1, \xi_2, \ldots\ldots$, we have

$$z_iz_k=\sum_{l=1}^{c}\gamma_{ikl}z_l\,, \qquad B^2=B\,.$$

Hence A is the sum of the algebras B and N. It was noted above that $A-N=B$ is a division algebra.

78. Principal theorem. *Any associative algebra A over a non-modular field F, which is neither semi-simple nor nilpotent, can be expressed as the sum of its maximal nilpotent invariant sub-algebra N and a semi-simple sub-algebra K over F, which is not a zero algebra of order* 1. *While K is not unique, any two determinations of it are equivalent.*

By § 57, A has a principal idempotent element u and

$$A=N_1+uAu\,, \qquad N_1\leqq N\,,$$

while if there is a maximal nilpotent invariant sub-algebra of uAu, it is contained in N. Hence our theorem will follow for A if proved for uAu, which has the modulus u.

It remains to prove the theorem for algebras A having a modulus. By § 38, $A-N$ is semi-simple and has a modulus.

First, let $A-N$ be simple. By § 55, $A=M\times B$, where M is a simple matric algebra and B is an algebra having a modulus, but no further idempotent element. By § 77, $B=D+N_1$, where D is a division algebra and N_1 is zero or the maximal nilpotent invariant sub-algebra of B. By § 56, $N=M\times N_1$. By § 52, $M\times D$ is simple and is not a zero algebra of order 1. Hence $A=M\times(D+N_1)$ is the sum of the simple algebra $M\times D$ and N.

Second, let $A-N$ be semi-simple, but not simple. By § 57, $A=N'+S$, where $N'\leqq N$ and S is the direct sum of algebras $A_1, \ldots, A_t$, where each A_i is of the type $M\times B$ just discussed and hence is the sum of a simple algebra K_i and N_i, where N_i is zero or the maximal nilpotent invariant sub-algebra of A_i if it exists. Moreover, $N=N'+\Sigma N_i$. Hence $A=K+N$, where $K=\Sigma K_i$ is a direct sum of simple algebras, no one a zero algebra of order 1, and hence is semi-simple and not a zero algebra of order 1 (§ 40).

79. Complex algebras. Any algebra over the field C of all complex numbers $a+bi$ is called *complex*.

A complex division algebra D is of order 1 and is generated by its modulus. For, if $f(\omega)=0$ is the equation of lowest degree satisfied by an element x of D, $f(\omega)$ is not a product of polynomials $f_1(\omega)$ and $f_2(\omega)$ each of degree $\geqq 1$, since $f_1(x)f_2(x)=0$ implies that one of $f_1(x)$ and $f_2(x)$ is zero in the division algebra D. But if $f(\omega)$ is of degree >1, it is a product of two or more linear

factors in C. Hence $f(\omega)$ is of degree 1 and x is the product of the modulus by a complex number.

Every complex simple algebra, not a zero algebra of order 1, is a simple matric algebra. For, by § 51, it is the direct product of a division algebra (here of order 1) by a simple matric algebra.

A complex semi-simple algebra which is not simple is a direct sum of simple matric algebras (§ 40).

The characteristic and rank equations of any semi-simple complex algebra are known by §§ 71, 72.

We are now in a position to give an elementary proof of the principal theorem that every complex algebra with a modulus is either semi-simple or is the sum of its maximal nilpotent invariant sub-algebra and a semi-simple sub-algebra. In the proof in § 78 of a more general theorem, use was made of the theorem in § 77 which may be proved far more simply for a complex algebra A. We may assume that the order of A is $r>1$. Then A is not simple since a simple matric algebra of order $r>1$ contains idempotent elements e_{ii} other than its modulus Σe_{ii}. In a semi-simple algebra which is not simple, the modulus of each component simple algebra is idempotent. Since A is not semi-simple, it has a maximal nilpotent invariant sub-algebra N. But $A-N$ is a complex division algebra (middle of § 77), which is therefore of order 1. Thus N is of order $r-1$. Hence A is the sum of N and the division algebra generated by the modulus of A.

For normalized basal units of any complex algebra, see chapter x.

CHAPTER IX

INTEGRAL ALGEBRAIC NUMBERS

80. Purpose of the chapter. We shall develop those properties of algebraic numbers which are essential in providing an adequate background for the theory of the arithmetic of any rational algebra to be presented in the next chapter. The latter theory will there be seen to be a direct generalization of the theory of algebraic numbers.

In order to make our presentation elementary and concrete, we shall develop the theory of quadratic numbers before taking up algebraic numbers in general.

81. Quadratic numbers. Let d be an integer, other than $+1$, which is not divisible by the square of any integer >1. As explained in § 1, the field $R(\sqrt{d})$ is composed of all rational functions of $\sqrt{d}$ with rational coefficients. Such a function can evidently be given the form

$$q=\frac{e+f\sqrt{d}}{g+h\sqrt{d}},$$

where e, f, g, h are rational numbers, and g and h are not both zero. Multiplying both numerator and denominator by $g-h\sqrt{d}$, in order to rationalize the denominator, we obtain $q=a+b\sqrt{d}$, where a and b are rational. Evidently q and $a-b\sqrt{d}$ are the roots of

$$x^2-2ax+(a^2-db^2)=0, \tag{1}$$

whose coefficients are rational. For this reason, q is called a *quadratic algebraic number.*

We shall assume that the coefficients of (1) are integers, and in that case call the root q a *quadratic integer.*

Then $2a$ and $4(a^2-db^2)$ are integers. Thus $4db^2$ is an integer. But d is an integer not divisible by a perfect square >1. Hence $4b^2$ has unity as its denominator, so that it and $2b$ are integers. Thus $a=\frac{1}{2}\alpha$, $b=\frac{1}{2}\beta$, where α and β are integers. Since a^2-db^2 shall be an integer, $\alpha^2-d\beta^2$ must be a multiple of 4.

If d is even, α^2 must be even and hence a multiple of 4. Thus also $d\beta^2$ must be a multiple of 4. But d is not divisible by the square 4. Hence β^2 is even. Thus α and β are both even. Hence, if d is even, q is a quadratic integer if and only if a and b are both integers.

If d is of the form $4k+3$, then $\alpha^2-d\beta^2$ and hence also $\alpha^2+\beta^2$ must have the remainder zero on division by 4. According as an integer is even or odd, its square has the remainder 0 or 1. Hence α and β are both even.

If d is of the form $4k+1$, then $\alpha^2-d\beta^2$, and hence also $\alpha^2-\beta^2$, must have the remainder zero on division by 4, so that α and β are both even or both odd. Hence $q=a+b\sqrt{d}$ is now a quadratic integer if and only if a and b are both integers or both halves of odd integers. These two cases may be combined by expressing q in terms of the quadratic integer θ defined by

$$\theta=\tfrac{1}{2}(1+\sqrt{d}), \qquad d=4k+1, \tag{2}$$

instead of in terms of $\sqrt{d}$ itself. First, if a and b are integers, then $x=a-b$ and $y=2b$ are integers and $q=x+y\theta$. Second, if $a=\frac{1}{2}(2r+1)$ and $b=\frac{1}{2}(2s+1)$ are halves of odd integers, then $x=r-s$ and $y=2s+1$ are integers and $q=x+y\theta$.

THEOREM 1. *If d is an integer $\neq 1$, not divisible by a square > 1, all quadratic integers of the field $R(\sqrt{d})$ are given by $x+y\theta$, where x and y are rational integers and $\theta=\sqrt{d}$ when d is of one of the forms $4k+2$, $4k+3$, while θ is defined by (2) when d is of the form $4k+1$.*

The quadratic integers of $R(\sqrt{d})$ are said to have the *basis* $1, \theta$ since they are all linear combinations of 1 and θ with integral coefficients x, y. Note that every number of the field is expressible as a linear combination $r \cdot 1 + s\theta$ with rational coefficients r, s.

THEOREM 2. *The sum, difference, or product of any two quadratic integers of the field $R(\sqrt{d})$ is a quadratic integer.*

For, if x, y, z, w are all integers, the sum of $q=x+y\theta$ and $t=z+w\theta$ is $r+s\theta$, where $r=x+z$ and $s=y+w$ are integers. Likewise, $q-t$ is a quadratic integer. Finally, the product qt is the sum of $xz+(xw+yz)\theta$ and $yw\theta^2$, and, by the previous result, will be a quadratic integer if θ^2, and hence also $yw\theta^2$, is one. The latter is evident if $\theta=\sqrt{d}$, and is true also for case (2) since then $\theta^2=\theta+k$, where $k=\frac{1}{4}(d-1)$ is an integer.

82. Algebraic numbers. We shall generalize the preceding concepts and theorems. When the coefficients of an algebraic equation are all rational numbers, the roots are called *algebraic numbers*. For an equation

$$x^n+a_1x^{n-1}+ \ldots . +a_n=0 \tag{3}$$

with integral coefficients, that of the highest power of x being unity, the roots are called *integral algebraic numbers*.

Note that any integer a is the root of the equation $x-a=0$ of type (3) and hence is an integral algebraic number.

THEOREM 3. *If an integral algebraic number α is a rational number, it is an integer.*

For, if $\alpha=b/d$, where b and d are integers without a common factor >1, and if α is a root of (3), then, by multiplying its terms by d^{n-1}, we get

$$\frac{b^n}{d}=-a_1b^{n-1}-a_2db^{n-2}-\ \ldots\ -a_nd^{n-1}.$$

Since the right member is an integer, we conclude that $d=\pm 1$. Hence $\alpha=\pm b$ is an integer.

We have the following generalization of Theorem 2:

THEOREM 4. *Any polynomial $f(\alpha, \beta, \ldots, \kappa)$ with integral coefficients in any integral algebraic numbers α, β, $\ldots$, κ is itself an integral algebraic number.*

For, let α be a root of equation $A(\alpha)=0$ of degree a, β a root of $B(\beta)=0$ of degree b, $\ldots$, and κ a root of $K(\kappa)=0$ of degree k, where each equation has integral coefficients, and the leading coefficient is unity. Write $n=ab\ldots k$ and denote by $\omega_1, \ldots, \omega_n$ the n numbers

$$\alpha^{a_1}\beta^{b_1}\ldots\kappa^{k_1} \qquad (a_1=0, 1, \ldots, a-1;\ b_1=0, 1, \ldots, b-1; \ldots),$$

arranged in any fixed order. By means of $A(\alpha)=0$, we can express $\alpha^a, \alpha^{a+1}, \ldots$ as polynomials in α of degree $<a$. Hence by means of $A(\alpha)=0, \ldots, K(\kappa)=0$, we can express the products $\omega_i f$ in the form

$$\omega_i f=c_{i1}\omega_1+c_{i2}\omega_2+\ \ldots\ +c_{in}\omega_n \qquad (i=1, \ldots n),$$

where each c_{ij} is a polynomial with integral coefficients in the coefficients of f, A, ... , K, so that each c_{ij} is an integer. Transposing the left members, we obtain n linear homogeneous equations in ω_1, ... , ω_n, the first step in the solution of which by determinants gives $D\omega_1 = 0$, ... , $D\omega_n = 0$, where

$$D = \begin{vmatrix} c_{11}-f & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22}-f & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{n1} & c_{n2} & \cdots & c_{nn}-f \end{vmatrix}.$$

Hence $D = 0$. Multiplying the expansion of D by $(-1)^n$, we get an equation $f^n + \ldots = 0$ with integral coefficients and leading coefficient unity. Thus f is an integral algebraic number.

83. Reducible polynomials. If we have an identity

$$f(x) \equiv f_1(x) f_2(x) \tag{4}$$

between three polynomials with rational coefficients such that f_1 and f_2 are of degrees less than the degree of f, we call $f(x)$ *reducible*. If no such identity exists, f is called *irreducible*.

THEOREM 5. *A reducible polynomial $f(x)$ with integral coefficients and leading coefficient unity is a product of two polynomials with integral coefficients and leading coefficient unity.*

By hypothesis, we have an identity (4). Let a be the coefficient of the highest power of x in f_1 and write $f_1 = ag(x)$, $f_2 = a^{-1}h(x)$. Then $f(x) \equiv g(x)h(x)$, where g and h have rational coefficients and have unity as the coefficient of the highest power of x.

The roots α_i of $f(x)=0$ are integral algebraic numbers. Certain of them, say $\alpha_1, \ldots, \alpha_r$, are the roots of $g(x)=0$, whence

$$g(x)\equiv(x-\alpha_1)(x-\alpha_2)\ \ldots\ (x-\alpha_r).$$

Computing the product of the factors, we see that the coefficients of g are equal to

$$1,\quad -(\alpha_1+\ \ldots\ +\alpha_r),\quad \alpha_1\alpha_2+\alpha_1\alpha_3+\ \ldots\ +\alpha_{r-1}\alpha_r,\quad \ldots,\quad (-1)^r\alpha_1\alpha_2\ \ldots\ \alpha_r,$$

which are therefore integral algebraic numbers by Theorem 4. But the coefficients of g are rational numbers. Hence by Theorem 3 these coefficients are integers. Similarly for the coefficients of h.

Theorem 5 is evidently equivalent to

GAUSS'S LEMMA. *If* $x^n+a_1x^{n-1}+\ \ldots\ .$ *has integral coefficients and is divisible by* $x^r+c_1x^{r-1}+\ \ldots\ +c_r$ *in which* $c_1, \ldots, c_r$ *are rational numbers, then* $c_1, \ldots, c_r$ *are integers*

84. Normal form of the numbers of an algebraic field. Consider the field $R(\alpha)$ composed of all rational functions with rational coefficients of a root α of an algebraic equation $A(x)=0$ with rational coefficients. In case $A(x)$ is reducible, it has an irreducible factor which vanishes when $x=\alpha$. Hence α satisfies an irreducible equation $f(x)=0$ of degree n with rational coefficients.

Any number of $R(\alpha)$ is by definition of the form

$$r(\alpha)=\frac{g(\alpha)}{h(\alpha)},\qquad h(\alpha)\neq 0, \tag{5}$$

where $g(x)$ and $h(x)$ are polynomials with rational coefficients. The usual process for finding the greatest com-

mon divisor $d(x)$ of $f(x)$ and $h(x)$ involves only multiplications and subtractions. Hence $d(x)$ has rational coefficients. Since $d(x)$ is a factor of the irreducible function $f(x)$, either $d(x)$ is a constant $c \neq 0$ or else is $cf(x)$. The latter alternative is here excluded, since it would imply that α is a root of $d(x) = 0$ and hence of $h(x) = 0$, contrary to (5). Hence we may take $d(x)$ to be 1. By I of § 113, the greatest common divisor $d(x)$ of $f(x)$ and $h(x)$ is expressible linearly in terms of them, whence

$$1 \equiv \sigma(x) \cdot f(x) + \tau(x) \cdot h(x),$$

where $\sigma(x)$ and $\tau(x)$ are polynomials with rational coefficients. Taking $x = \alpha$ in this identity, we get $1 = \tau(\alpha)h(\alpha)$. Hence (5) gives $r(\alpha) = g(\alpha)\tau(\alpha)$. From this product we may eliminate $\alpha^n, \alpha^{n+1}, \ldots$ by means of $f(\alpha) = 0$ and obtain

$$(6) \qquad r(\alpha) = r_0 + r_1\alpha + r_2\alpha^2 + \ldots + r_{n-1}\alpha^{n-1},$$

in which the coefficients r_i are rational numbers.

If there were two such expressions (6) for $r(\alpha)$, the coefficients of like powers of α must be equal. For, if not, α would satisfy an equation $h(x) = 0$ with rational coefficients whose degree is $\leqq n - 1$. Then the greatest common divisor $d(x)$ of f and h is not a constant (in view of the common root α) and hence would be $cf(x)$, as shown above. But $cf(x)$ is of degree n and is not a divisor of $h(x)$.

THEOREM 6. *If α is a root of an irreducible equation of degree n with rational coefficients, every number of the field $R(\alpha)$ can be expressed in one and but one way in the normal form* (6). *The field is said to be of degree n.*

For $n=2$, this theorem was proved very simply in § 81.

The final step in the foregoing proof led to the useful result:

THEOREM 7. *If two equations* $h(x)=0$ *and* $f(x)=0$ *with rational coefficients have a root in common, and if* $f(x)$ *is irreducible, then* $f(x)$ *is an exact divisor of* $h(x)$.

COROLLARY. *An irreducible equation* $f(x)=0$ *with rational coefficients has no multiple root.*

For, it would then have a root in common with $f'(x)=0$.

85. Normal form of the integral algebraic numbers of a field. Consider any algebraic field $R(a)$, where a is a root of an irreducible equation

$$x^n+a_1x^{n-1}+ \ldots . +a_n=0$$

with rational coefficients. We may express $a_1, \ldots . , a_n$ as fractions with the common denominator d, where d and the numerators are all integers. Then

$$(da)^n+da_1(da)^{n-1}+ \ldots . +d^na_n=0,$$

so that $\theta=da$ is a root of an equation $f(x)=0$ with integral coefficients da_1. $d^2a_2, \ldots . , d^na_n$, and leading coefficient unity. Hence θ is an integral algebraic number belonging to $R(a)$. Evidently our field is identical with $R(\theta)$.

By § 84, each number of $R(\theta)$ may be given the form

$$\rho=r_0+r_1\theta+r_2\theta^2+ \ldots . +r_{n-1}\theta^{n-1}, \tag{7}$$

where the r_i are rational numbers.

Let $\theta_1, \ldots, \theta_{n-1}$ be the remaining roots of the foregoing irreducible equation $f(x)=0$ satisfied by θ, and write

$$(8)\quad \begin{cases} \rho_1 = r_0+r_1\theta_1+r_2\theta_1^2+\ldots+r_{n-1}\theta_1^{n-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \rho_{n-1}=r_0+r_1\theta_{n-1}+r_2\theta_{n-1}^2+\ldots+r_{n-1}\theta_{n-1}^{n-1}. \end{cases}$$

The coefficients of the polynomial form $\phi(y)$ of the product

$$(y-\rho)(y-\rho_1)\ldots(y-\rho_{n-1})$$

are symmetric functions, with rational coefficients, of the roots $\theta, \theta_1, \ldots, \theta_{n-1}$ of $f(x)=0$, having integral coefficients, and hence are equal to rational numbers.

Let $\lambda(y)=0$ be the irreducible equation with rational coefficients and leading coefficient unity which has the root ρ. By Theorem 7, $\phi(y)$ is divisible by $\lambda(y)$. Unless $\phi\equiv\lambda$, the quotient $q(y)$ of ϕ by λ vanishes for one of $\rho, \rho_1, \ldots, \rho_{n-1}$ and hence for ρ itself as we shall next prove. For, if $q(\rho_i)=0$, $q(r_0+r_1z+r_2z^2+\ldots)$ vanishes for $z=\theta_i$ and hence by Theorem 7 has the factor $f(z)$ and therefore vanishes for $z=\theta$. This proves that $q(y)$ vanishes for $y=\rho$, and hence has the factor $\lambda(y)$. Proceeding as before with the present quotient, we see in this way that $\phi(y)$ is an exact power of $\lambda(y)$.

We now assume that ρ is an integral algebraic number, so that it satisfies an equation $\mu(y)=0$ with integral coefficients and leading coefficient unity. Then, by Theorem 7, $\mu(y)$ is divisible by the irreducible function $\lambda(y)$ which also vanishes for $y=\rho$. By Gauss's lemma (§ 83), the coefficients of $\lambda(y)$ are all integers. The same is therefore true of its exact power $\phi(y)$. The latter vanishes for $\rho, \rho_1, \ldots, \rho_{n-1}$, which are therefore integral algebraic numbers.

The determinant of the coefficients of $r_0, r_1, \ldots, r_{n-1}$ in (7) and (8) is

$$\Delta = \begin{vmatrix} 1 & \theta & \theta^2 & \ldots & \theta^{n-1} \\ 1 & \theta_1 & \theta_1^2 & \ldots & \theta_1^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \theta_{n-1} & \theta_{n-1}^2 & \ldots & \theta_{n-1}^{n-1} \end{vmatrix}. \tag{9}$$

By the interchange of any two of $\theta, \theta_1, \ldots, \theta_{n-1}$, the corresponding two rows of Δ are interchanged, so that Δ becomes $-\Delta$, and Δ^2 is unaltered. In other words, Δ^2 is a symmetric function of the roots $\theta, \theta_1, \ldots$ of the equation $f(x) = 0$ having integral coefficients and leading coefficient unity. Hence* Δ^2 is an integer d.

It is easy to factor the determinant Δ in which, for the moment, we regard $\theta, \theta_1, \ldots$ as independent variables. If $\theta = \theta_1$, the first two rows are alike and Δ vanishes, whence Δ has the factor $\theta - \theta_1$. In this way, and by counting the total degree in $\theta, \theta_1, \ldots$, we see that Δ^2 is the product of the squares of the differences of $\theta, \theta_1, \ldots, \theta_{n-1}$, so that d is the discriminant of $f(x) = 0$. Hence, by the corollary in § 84, *the integer d is not zero.*

We now solve equations (7) and (8) for r_s by the usual method of determinants. Denote by Δ_s the determinant obtained from Δ by replacing the elements $\theta^s, \theta_1^s, \ldots$ of the $(s+1)$th column by the left members $\rho, \rho_1, \ldots$. Hence, $\Delta r_s = \Delta_s$. Thus $dr_s = \Delta\Delta_s \equiv c_s$. Since c_s is a rational number dr_s, and is also a polynomial $\Delta\Delta_s$ with integral coefficients in the integral algebraic numbers $\theta, \theta_1, \ldots, \theta_{n-1}, \rho, \rho_1, \ldots, \rho_{n-1}$ and hence is itself an integral algebraic number by Theorem 4,

* Dickson's *First Course in the Theory of Equations* (1922), p. 130.

it follows from Theorem 3 that c_s is an integer. From $r_s = c_s/d$ and (7), we get

$$\rho = (c_0 + c_1\theta + c_2\theta^2 + \ldots + c_{n-1}\theta^{n-1})/d. \tag{10}$$

THEOREM 8. *Every algebraic field of degree n is identical with the field $R(\theta)$ defined by one of its integral algebraic numbers θ. Every integral algebraic number of $R(\theta)$ can be expressed in one and only one way in the normal form* (10), *where $c_0, \ldots, c_{n-1}$ are integers, while d is a fixed integer $\neq 0$ determined by θ. In fact, d is the discriminant of the irreducible equation satisfied by θ and having integral coefficients and leading coefficient unity.*

86. Basis. We shall prove the following generalization of Theorem 1:

THEOREM 9. *In any algebraic field $R(\theta)$ of degree n there exist n integral algebraic numbers $\omega_1 = 1, \omega_2, \ldots, \omega_n$ such that every integral algebraic number ρ of the field is expressible in one and only one way in the form*

$$\rho = q_1\omega_1 + \ldots + q_n\omega_n, \tag{11}$$

where $q_1, \ldots, q_n$ are integers. Then $\omega_1, \ldots, \omega_n$ are said to form a **basis** *of the integral algebraic numbers of the field.*

Since the proof* applies also to the analogous question for a rational algebra in place of our field (§ 95), we shall employ a notation suitable to both situations. Accordingly, we write $u_1 = 1$, $u_2 = \theta$, $u_3 = \theta^2$, $\ldots$, $u_n = \theta^{n-1}$. Then every integral algebraic number (10) of the field may be given the notation

* For a geometric proof see Minkowski, *Diophantische Approximationen* (1907), p. 123.

$$(12) \qquad \rho=(a_1u_1+a_2u_2+ \ . \ . \ . \ . \ +a_nu_n)/d,$$

where $a_1, \ . \ . \ . \ . \ , a_n$ are integers.

First, the integral algebraic numbers (12) having $a_2=0, \ . \ . \ . \ . \ , a_n=0$ are rational numbers a_1/d and hence are integers by Theorem 3. Thus they are products of $\omega_1=1$ by integers q_1 and hence are of the form (11).

Second, the integral algebraic numbers* (12) having $a_2\neq 0$ and $a_3=0, \ . \ . \ . \ . \ , a_n=0$ may be denoted by

$$(13) \quad \omega_2=\frac{au_1+bu_2}{d}, \qquad \omega_2'=\frac{a'u_1+b'u_2}{d},$$

$$\omega_2''=\frac{a''u_1+b''u_2}{d}, \ . \ . \ . \ . \ .$$

The greatest common divisor of $b, \ b', \ b'', \ . \ . \ . \ .$ is a function $cb+c'b'+ \ . \ . \ . \ .$ of them with integral coefficients $c, \ c', \ . \ . \ . \ .$ (I, § 113). Hence $c\omega_2+c'\omega_2'+ \ . \ . \ . \ .$ is an integral algebraic number of the field and therefore is one of the numbers (13) lacking $u_3, \ . \ . \ . \ . \ , u_n$. We may assume that it is the first one ω_2, since the arrangement of the numbers (13) is immaterial. Hence b is a divisor of $b', \ b'', \ . \ . \ . \ .$ in (13).

Similarly, for any $i\leqq n$, the integral algebraic numbers (12) having $a_i\neq 0, \ a_{i+1}=0, \ . \ . \ . \ . \ , a_n=0$ [including certainly all numbers (12) in which also $a_1, \ . \ . \ . \ . \ , a_i$ are integral multiples of d] may be denoted by

$$\omega_i=(b_1u_1+ \ . \ . \ . \ . \ +b_iu_i)/d,$$

$$\omega_i'=(b_1'u_1+ \ . \ . \ . \ . \ +b_i'u_i)/d, \ . \ . \ . \ . \ .$$

As before, we may assume that b_i is the greatest common divisor of $b_i, \ b_i', \ . \ . \ . \ . \ .$

* There exist such numbers, for example, $r+s\theta$, where r and s are integers, which is obtained by taking $a_1=rd, \ a_2=sd, \ a_i=0 \ (i>2)$.

The resulting numbers $\omega_1, \ldots, \omega_n$ form a basis. For, every integral algebraic number ρ of the field is of the form (12). Then, if

$$\omega_{n-1}=(g_1u_1+ \ldots + g_{n-1}u_{n-1})/d,$$
$$\omega_n=(h_1u_1+ \ldots + h_nu_n)/d,$$

h_n is a divisor of a_n; let q_n be the quotient. Hence

$$\rho_1=\rho-q_n\omega_n$$

lacks u_n and is therefore of the form

$$\rho_1=(l_1u_1+ \ldots + l_{n-1}u_{n-1})/d.$$

Similarly, g_{n-1} is a divisor of l_{n-1}; let q_{n-1} be the quotient. Hence $\rho_2=\rho_1-q_{n-1}\omega_{n-1}$ lacks both u_{n-1} and u_n. Proceeding in this manner, we see that

$$\rho-q_n\omega_n-q_{n-1}\omega_{n-1}- \ldots - q_1\omega_1$$

lacks $u_1, \ldots, u_n$ and hence is zero. This proves (11).

COROLLARY. *Every number α of the field is expressible in one and only one way in the form* (11), *where* $q_1, \ldots, q_n$ *are now merely rational numbers.*

For, by the first part of § 85, the product of α by a suitably chosen integer is an integral algebraic number, so that the product is a linear function of the ω's with integral coefficients.

CHAPTER X

THE ARITHMETIC OF AN ALGEBRA

We shall develop a simple theory of the integral elements of any algebra, thereby generalizing the classic theory of integral algebraic numbers. The older definitions of the integral elements of an algebra are shown to be wholly unsatisfactory; not a single general theorem was obtained from them.

We shall develop early Hurwitz' theory of integral quaternions in a much simplified form in order that the reader may understand from a concrete example the nature and properties of the arithmetic of an algebra. We shall then develop the remarkable new theory for any algebra, an outline of which is given in § 92.

This theory furnishes a new method of solving completely various types of Diophantine equations, which have not been solved by other methods; lack of space restricts us to a single typical illustration (§ 106).

87. Integral elements, case of algebraic numbers. Let A be any associative algebra, having a modulus designated by 1, over the field of rational numbers. Each element of a set of elements of A shall be called an *integral element* if the set has the following four properties:

R (rank equation): For every element of the set, the coefficients of the rank equation* are all integers

C (closure): The set is closed under addition, subtraction, and multiplication.

* The coefficient of the highest power of the unknown is always 1 (§ 69). By an integer is meant a whole number.

U (unity): The set contains the modulus 1.

M (maximal): The set is a maximal (i.e., it is not contained in a larger set having properties R, C, U).

Some reasons are indicated in the footnote of § 96 why it might be desirable to require also the property that each set shall be of the same order as A; this property is actually assumed only in § 97.

We proceed to illustrate this definition for the important case in which the algebra is any algebraic field $R(\theta)$ of degree n. By the theorem and corollary of § 86, that field contains n integral algebraic numbers $u_1=1, u_2, \ldots, u_n$ such that every integral algebraic number x of the field is expressible in one and but one way in the form

$$x=\xi_1 u_1+\ldots+\xi_n u_n, \tag{1}$$

where $\xi_1, \ldots, \xi_n$ are integers, while every number x of the field is expressible in one and only one way in the same form (1), where now the ξ_i are merely rational numbers.

By Theorem 4 of § 82, the product of two integral algebraic numbers u_i and u_j is an integral algebraic number. Hence by the preceding result,

$$u_i u_j=\sum_{k=1}^{n}\gamma_{ijk}u_k \qquad (i, j=1, \ldots, n), \tag{2}$$

where each γ is an integer. The field $R(\theta)$ is therefore an algebra of order n over the field R of all rational numbers with the set of basal units $u_1, \ldots, u_n$ and multiplication table (2).

By § 60, x is a root of the first characteristic equation $\delta(\omega)=0$ of degree n. When the co-ordinates ξ_i of x in (1) are arbitrary rational numbers, $\delta(\omega)$ has rational coefficients and is irreducible in R. For, if reducible, it would continue to be reducible when we give to the ξ_i the values of the co-ordinates of θ, whereas θ was assumed to satisfy an equation of degree n irreducible in R and hence, by Theorem 7 of § 84, θ satisfies no equation of degree $<n$ with rational coefficients. This proves that the rank equation is $(-1)^n\delta(\omega)=0$.

The coefficients of $\delta(\omega)$ are polynomials in the ξ_i and the γ_{ijk} with integral coefficients and hence are integers when the ξ_i are all integers, i.e., when x in (1) is an integral algebraic number.

Hence the set S of all integral algebraic numbers of any algebraic field $R(\theta)$ has property R. It has property U since $u_1=1$. It has property C by Theorem 4 of § 82.

Next, any set of numbers x of the field $R(\theta)$ which has properties R, C, U is either S or a sub-set of it. For, by R, the coefficients of the rank equation of x are integers and the coefficient of the highest power of the unknown is unity (§ 69). Hence x is an integral algebraic number.

Thus S is the unique maximal set.

THEOREM. *If an algebra is an algebraic field, its unique maximal set of integral elements is composed of all the integral algebraic numbers of the field.*

88. Units, associated elements, and arithmetics. Two integral elements of an algebra A whose product is the modulus 1 are called *units* of A. Any product of units is a unit. For, $uu_1=vv_1=ww_1=1$ imply $uvw\cdot w_1v_1u_1=1$.

If x is an integral element and if u is a unit, then xu and ux are called *right* and *left associates* of x, respectively. If also u' is a unit, x is said to be *associated* with uxu'. Associated elements play equivalent rôles in questions of divisibility. For instance, if also v and w are units whose product is 1, $x=yz$ implies $uxu'=uyv\cdot wzu'$.

For example, if $i=\sqrt{-1}$, the field $R(i)$ is a rational algebra of order 2 whose integral elements are $x=a+bi$, where a and b are integers (§ 81). Then x is a unit if its product by $a-bi$ is unity. There are exactly four units, viz., ± 1, $\pm i$. The four associates of x are $\pm x$ and $\pm ix=\mp(b-ai)$.

If in an algebra A the integral elements whose determinant* is not zero may be associated in the foregoing sense with the various integral elements of a subalgebra, we shall say that the latter elements form an arithmetic *associated* with the arithmetic of A.

89. Example. Consider the rational algebra A with two basal units 1 and e, where $e^2=0$. The rank equation of $x=a+be$ is $(x-a)^2=0$, whose coefficients are integers if and only if a is integral. The unique maximal set of elements having properties R, C, U is evidently composed of the $x=a+be$ in which a is integral and b is rational. Every such x is therefore an integral element of A.

For any rational k, $u=1+ke$ is a unit since its product by another integral element $1-ke$ is 1.

Let $a\neq 0$ and take $k=-b/a$. Then $xu=a$. Hence if the determinant a^2 of x is not zero, x is associated with the integer a. Thus x can be decomposed into primes in only one way apart from unit factors.

* Either $\Delta(x)$ or $\Delta'(x)$ may be understood since both are simultaneously not zero or both zero by the footnote in § 58.

Hence the arithmetic of algebra A is associated with the ordinary arithmetic of integers.

This result illustrates the fundamental theorem (§ 104) that the arithmetic of A is associated with that of the sub-algebra whose elements are derived by suppressing the components (here be) which belong to the maximal nilpotent invariant sub-algebra of A.

90. Failure of earlier definitions of arithmetics. Du Pasquier* defined a set of integral elements of a rational algebra A to be one having properties C, U, M, and (in place of R)

B. The set has a finite basis (i.e., it contains elements $q_1, \ldots, q_k$ such that every element of the set is expressible in the form $\Sigma c_i q_i$, where each c_i is an integer)

We shall test this definition by the special algebra in § 89. Then any set having properties B, C, U is readily seen to have a basis $1, q=r+se$, where r and s are fixed rational numbers and $s\neq 0$. Since q^2 is in the set by property C, we must have $q^2=a+bq$, where a and b are integers. This equation is equivalent to

$$r^2=a+br, \qquad 2rs=bs.$$

Hence $2r=b$, $r^2=-a$. If the rational number r were not integral, its square would not be equal to the integer $-a$. Since r is integral, the basis $1, q$ may be replaced by $1, q-r$. Hence every set has a basis of the form $1, se$, where s is rational and $\neq 0$.

This set, designated by $(1, se)$, is evidently contained in the larger set $(1, \frac{1}{2}se)$, which in turn is contained in the still larger set $(1, \frac{1}{4}se)$, etc. Hence there is no maximal

* *Vierteljahrsschrift Naturf Gesell. Zürich*, LIV (1909), 116–48; *L'enseignement math.*, XVII (1915), 340–43; XVIII (1916), 201–60.

set. In other words, the algebra does not possess integral elements.

Suppose we omit the requirement M and define the integral elements of our algebra to be those of any chosen one of the infinitude of non-maximal sets. It has been proved by the author* that factorization into indecomposable integral elements is not unique and cannot be made unique by the introduction of ideals however defined.

The same insurmountable difficulties arise for sets having properties B, C, U′, M, where † U′ requires that the set shall contain all the basal units, one of which is the modulus (1 and e in our example). This definition was employed by A. Hurwitz for the arithmetic of quaternions (§ 91). Since now e shall occur in the set $(1, se)$, s must be the reciprocal of an integer. Then also $\frac{1}{2}s$, $\frac{1}{4}s$, ... are reciprocals of integers. Hence $(1, \frac{1}{2}se)$ is a set containing $(1, se)$, and as before there is no maximal set.

Note that the aggregate of the elements in the infinitude of sets $(1, se)$ obtained by the definition given by either Du Pasquier or Hurwitz is the set of integral elements obtained in § 89 by the new definition. This suitable enlargement of each of their sets enabled us to overcome their serious difficulties. This is analogous to the gain by each of the successive enlargements of the primitive set of positive integers to the set of positive

* *Journal de Mathématiques*, Series 9, Vol. II (1923). Also that similar insurmountable difficulties arise for many other algebras under the definition by Du Pasquier.

† Unlike properties R, C, U, B, property U′ is not preserved under every transformation of the basal units. Hence U′ is not a desirable assumption.

and negative integers, then to the field of all rational numbers, then to the field of all real numbers, and finally to the field of all complex numbers.

91. Arithmetic of quaternions.* By § 11, $q=\sigma+\xi i+\eta j+\zeta k$ and its conjugate $q'=\sigma-\xi i-\eta j-\zeta k$ are the roots of

$$(3)\quad \omega^2-2\sigma\omega+N(q)=0, \qquad N(q)=qq'=\sigma^2+\xi^2+\eta^2+\zeta^2.$$

Since the coefficients of the rank equation (3) are integers when σ, ξ, η, ζ are integers, the set I of all quaternions having integral co-ordinates has the properties R, C, U.

We seek every set S of rational quaternions q which has properties R, C, U and which contains I and hence $1, i, j, k$. By R and (3), $N(q)$ and the double 2σ of the scalar part σ of q are both integers. By C, the set contains iq, jq, kq, whose scalar parts are $-\xi$, $-\eta$, $-\zeta$. As before, their doubles are integers. Hence $4N$ is the sum of the squares of four integers. That sum is divisible by 4 since N is an integer. But the square of an even or odd integer has the respective remainder 0 or 1 when divided by 4, and a sum of four such remainders is a multiple of 4 only when they are all 0 or all 1. Hence the co-ordinates of q are either all integers or all halves of odd integers. In either case the difference of any two co-ordinates is an integer. Thus every quaternion in S is of the form

$$q=\sigma+(\sigma+x_1)i+(\sigma+x_2)j+(\sigma+x_3)k,$$

* A much more complicated theory, based on an earlier definition (§ 90), was given by A. Hurwitz, *Göttinger Nachrichten* (1896), pp. 311–40; and amplified in his book, *Vorlesungen über die Zahlentheorie der Quaternionen* (Berlin, 1919).

where each x_i is an integer. Write x_0 for the integer 2σ. Then

$$(4) \qquad q=x_0\rho+x_1i+x_2j+x_3k, \qquad \rho=\tfrac{1}{2}(1+i+j+k).$$

Conversely, all such quaternions q in which $x_0, \ldots, x_3$ are integers form a set S having properties R, C, U. This is true as to R by what precedes, and as to U since (4) becomes 1 for $x_0=2$, $x_1=x_2=x_3=-1$. To prove C, it suffices to prove that the squares and products by twos of ρ, i, j, k all belong to S. By (3), $\rho^2-\rho+1=0$, so that ρ^2 is in S. Next,

$$i\rho=\tfrac{1}{2}(-1+i-j+k), \qquad \rho i=\tfrac{1}{2}(-1+i+j-k)$$

have all co-ordinates equal to halves of odd integers and hence are in S. The same is true of $j\rho$, ρj, $k\rho$, ρk, as shown by permuting i, j, k cyclically, which leaves unaltered the multiplication table of i, j, k given in § 11.

Hence this set S is the unique maximal of all sets having properties R, C, U, and containing i, j, k. This set S will be shown to give such a remarkably simple arithmetic that we shall call its quaternions integral without inquiring whether there exist further maximal sets.

THEOREM 1. *The integral quaternions are given by* (4) *for integral values of* $x_0, \ldots, x_3$. *Expressed otherwise, they are the quaternions whose four co-ordinates are either all integers or all halves of odd integers.*

LEMMA 1. *Given any real quaternion* h *and any positive integer* m, *we can find an integral quaternion* q *such that* $N(h-mq)<m^2$.

Express q in the form (4) and likewise write

$$h=h_0\rho+h_1 i+h_2 j+h_3 k\,.$$

Inserting the value of ρ from (4), we see that h has the co-ordinates $\frac{1}{2}h_0$, $\frac{1}{2}(h_0+2h_t)$ for $t=1, 2, 3$. Similarly, the co-ordinates of $h-mq$ are

$$\tfrac{1}{2}(h_0-mx_0)\,, \qquad \tfrac{1}{2}\{h_0+2h_t-mx_0-2mx_t\} \qquad (t=1, 2, 3).$$

These can be made numerically $\leqq\frac{1}{4}m$, $\frac{1}{2}m$, respectively, by choice of integers x_0, x_t. Then

$$N(h-mq)\leqq(\tfrac{1}{4}m)^2+3(\tfrac{1}{2}m)^2=\tfrac{1}{16}m^2<m^2\,.$$

LEMMA 2. *Given any integral quaternions a and b, $b\neq 0$, we can find integral quaternions q, c, Q, C such that*

$$a=qb+c\,, \qquad N(c)<N(b)\,, \tag{5}$$

$$a=bQ+C\,, \qquad N(C)<N(b)\,. \tag{6}$$

To obtain (5), apply Lemma 1 for $h=ab'$, $m=bb'$, where b' is the conjugate of b. Then $h-mq=(a-qb)b'$ has the norm $N(a-qb)\cdot N(b)<m^2$. Writing c for the integral quaternion $a-qb$, we get (5).

To obtain (6), apply Lemma 1 for $h=b'a$, $m=b'b$, $q=Q$, and write C for $a-bQ$.

If a, b, and q are integral quaternions such that $a=qb$, then a is said to have b as a *right divisor* and q as a *left divisor*. If also $b=hc$ has the right divisor c, then $a=qh\cdot c$ has the right divisor c.

Two integral quaternions a and b are said to have a *greatest common right divisor* D if D is a right divisor of both a and b and if every common right divisor of them

is a right divisor of D. The word *right* may be replaced by *left* throughout.

THEOREM 2.* *Any two integral quaternions a and b, not both zero, have a greatest common right divisor D which is determined uniquely up to a unit left factor, and $D=Aa+Bb$, where A and B are integral quaternions. Similarly, there exists a greatest common left divisor δ, unique up to a unit right factor, and $\delta=a\alpha+b\beta$.*

For, if $c\neq 0$ in (5), we may apply Lemma 2 to b and c in place of a and b, and get $b=q_1c+d$, where q_1 and d are integral quaternions for which $N(d)<N(c)$. If $d\neq 0$, we repeat the process on c and d. Since $N(b)$, $N(c)$, $N(d)$, ... form a series of decreasing integers $\geqq 0$, the process terminates and we reach a quaternion whose norm is zero and hence is itself zero. To simplify the notations, let this happen at the fourth step, so that

$$(7)\quad a=qb+c,\quad b=q_1c+d,\quad c=q_2d+D,\quad d=q_3D,\quad D\neq 0.$$

These equations, taken in reverse order, evidently imply that D is a right divisor of d, c, b, and a.

Conversely, let δ be any right divisor of both $a=\alpha\delta$ and $b=\beta\delta$. Then (7) show that δ is a right divisor of c, d, and D.

* In *Proceedings of the London Mathematical Society*, Series 2, Vol. XX (1921), pp. 225–32, Dickson called a quaternion integral if and only if its co-ordinates are all integers and proved Theorem 2 under the restriction that at least one of a and b is of odd norm, after proving Lemma 1 with m odd. The further theory holds unchanged. The object was to avoid the troublesome denominators 2 in applying the theory to the solution of equations in integers (§ 106). The same definition of integral quaternions had been used by R. Lipschitz in his very complicated theory based on quadratic congruences, *Untersuchungen über die Summen von Quadraten* (Bonn, 1886); French translation in *Journal de Mathématiques*, Sér. 4, Tome II (1886) 393–439.

Hence by definition D is a greatest common right divisor of a and b. As to the uniqueness of D, let E be another greatest common right divisor of a and b. Then D and E are right divisors of each other, so that $D=rE$, $E=sD$, where r and s are integral quaternions. Then $D=rsD$, $1=rs$, so that r and s are units (§ 88).

Writing l for $1+q_2q_1$, we obtain from (7)

$$D=c-q_2d=lc-q_2b=l(a-qb)-q_2b=la+(-lq-q_2)b.$$

This completes the proof of the first part of Theorem 2.

Two integral quaternions a and b are called right-handed *relatively prime* if and only if their greatest common right divisor is a unit, the condition being the existence of integral quaternions A and B such that $Aa+Bb=1$.

LEMMA 3. *An integral quaternion a whose norm is divisible by an integer $p>1$ has in common with p a right (and a left) divisor not a unit.*

For, if there be no such common divisor, a and p would be relatively prime, so that there would exist integral quaternions A and B satisfying $Aa+Bp=1$. Then

$$\begin{aligned} N(A)N(a)=N(1-Bp)&=(1-Bp)(1-B'p)\\ &=1-(B+B')p+BB'p^2=1+tp, \end{aligned}$$

where t is an integer. But $N(a)$ is divisible by p.

LEMMA 4. *If p is a prime there exist integral solutions of*

$$1+x^2+y^2\equiv 0 \pmod{p}. \tag{8}$$

For $p=2$, we may take $x=1$, $y=0$. Let $p>2$. If -1 is a quadratic residue of p, so that $-1\equiv x^2 \pmod p$, we may take $y=0$. Next, let -1 be a quadratic non-residue of p, and let a denote the first quadratic residue of p in the series $p-1, p-2, p-3, \ldots$, the final term 1 being certainly a quadratic residue. Then $b=a+1$ is a quadratic non-residue. The product of any two quadratic non-residues is known to be a quadratic residue. Hence $-b$, as well as a, is a quadratic residue. In other words, there exist integers x and y for which $a\equiv x^2$, $-a-1=-b\equiv y^2 \pmod p$. These imply (8).

An integral quaternion, not a unit, is called a *prime quaternion* if it admits only such representations as a product of two integral quaternions in which one of them is a unit. If π is a prime quaternion and if u and v are any units, then $u\pi v$ is a prime quaternion, since if it were a product ab, then $\pi=u'a\cdot bv'$.

LEMMA 5. *A prime p is not a prime quaternion.*

For, by Lemma 4, there exists an integral quaternion $q=1+xi+yj$ whose norm is divisible by p. Hence by Lemma 3 there exists a common right divisor d, not a unit, of $p=Pd$ and $q=Qd$. If P were a unit, so that $P'P=1$, then $q=(QP')p$. But this product of the integral quaternion QP' by p has all co-ordinates multiples of p, whereas the first co-ordinate of q is 1. This contradiction shows that P is not a unit, so that $p=Pd$ is a product of two integral quaternions neither of which is a unit.

LEMMA 6. *If the norm of an integral quaternion π is a prime, then π is a prime quaternion.*

For, if $\pi=ab$, $N(a)N(b)=N(\pi)$ is a prime, so that either $N(a)=1$ or $N(b)=1$, whence either a or b is a unit.

THEOREM 3. *Every prime quaternion π arises from the factorization $p=\pi\pi'$ of a prime p. Conversely, every prime p is a product of two conjugate prime quaternions.*

For, if π is a prime quaternion, and p is a prime dividing the integer $N(\pi)>1$, there exists by Lemma 3 an integral quaternion d, not a unit, such that $\pi=ud$, $p=Pd$. Here u is a unit by the definition of a prime quaternion π, so that $u'u=1$. Hence

$$u'\pi=d, \qquad p=Pu'\pi, \qquad p^2=N(P)N(\pi), \qquad N(\pi)\neq 1.$$

Either $p=N(\pi)=\pi\pi'$, as desired, or $p^2=N(\pi)$, $N(P)=1$. Then P and $v=Pu'$ are units, so that $p=v\pi$ is a prime quaternion, contrary to Lemma 5.

To prove the second part of Theorem 3, note that, by the proof of Lemma 5, $p=Pd$, where neither P nor d is a unit. Thus $N(P)=N(d)=p$. By Lemma 6, P is a prime quaternion.

LEMMA 7. *Given any integral quaternion a, we can find a unit* u such that au has integral co-ordinates.*

For, if a itself has integral co-ordinates, take $u=1$. In the contrary case, $a=\frac{1}{2}(a_0+a_1i+\ \ldots\ )$, where each a_t is an odd integer by Theorem 1. Thus $a_t=4n_t+r_t$, where $r_t=1$ or -1. Then

$$a=2n+r, \qquad n=n_0+n_1i+\ \ldots\ , \qquad r=\tfrac{1}{2}(r_0+r_1i+\ \ldots\ ).$$

Since r is an integral quaternion whose norm is $4(\frac{1}{2})^2=1$, r is a unit. We take $u=r'$. Then $au=2nr'+1$, whose co-ordinates are all integers.

* The twenty-four units, obtained from $N(u)=1$, are

$$\pm 1, \ \pm i, \ \pm j, \ \pm k, \qquad \tfrac{1}{2}(\pm 1\pm i\pm j\pm k).$$

This enumeration will be used only to distinguish the arithmetic of quaternions from that of an algebra discussed later.

THEOREM 4. *Every positive integer is a sum of four integral squares.*

This will follow if proved for primes since the product of any two sums of four integral squares is expressible as a sum of four integral squares in view of $N(q)N(Q) = N(qQ)$. If p is a prime, Theorem 3 shows that $p = PP'$, where P and P' are conjugate prime quaternions. By Lemma 7, $P = Qu$, where Q has integral co-ordinates and u is a unit. Then $P' = u'Q'$, $uu' = 1$, whence $p = QQ'$ is a sum of four integral squares.

LEMMA 8. *If q is an integral quaternion whose norm is even, then $q = (1+i)h$, where h is an integral quaternion.*

For, the square of half an odd integer is of the form $\frac{1}{4}(8m+1)$ and the sum of four such squares is odd. Hence the four co-ordinates q_s of q are all integers such that

$$0 \equiv \Sigma q_s^2 \equiv \Sigma q_s \pmod 2.$$

Thus q_1+q_0 and q_3+q_2 have an even sum and are therefore both even or both odd. In the respective cases, the co-ordinates of

$$h = \tfrac{1}{2}(q_1+q_0) + \tfrac{1}{2}(q_1-q_0)i + \tfrac{1}{2}(q_3+q_2)j + \tfrac{1}{2}(q_3-q_2)k$$

are all integers or all halves of odd integers, whence h is an integral quaternion. But $(1-i)q = 2h$, whence $q = (1+i)h$.

THEOREM 5. *Any integral quaternion can be given the form $(1+i)^r mcv$, where m is an integer, v is a unit, and c is a quaternion of odd norm whose co-ordinates are integers without a common factor >1. Let $N(c) = pql\ldots$, where $p, q, l, \ldots$ are the prime factors, not necessarily distinct, of $N(c)$ arranged in an arbitrarily*

chosen order. Then $c=\pi\kappa\lambda\ldots\ldots$, *where* $\pi, \kappa, \lambda, \ldots\ldots$ *are prime quaternions of norms* $p, q, l, \ldots\ldots$, *respectively. Here* π *may be chosen as any one of a certain set of right-hand associated quaternions, and then* κ *may be chosen as any one of another such set, etc. There are no further decompositions of* c *into prime quaternions whose norms are* $p, q, l, \ldots\ldots$ *in that order.**

For, by Lemma 8, we may express the given quaternion in the form $(1+i)^r a$, where a is an integral quaternion whose norm is odd. By Lemma 7, we can choose a unit u such that $au=b$ has integral co-ordinates, whence $a=bv$, where $v=u'$ is a unit. Let m be the greatest common divisor of the co-ordinates of b, and write $b=mc$. This proves the first statement in the theorem.

By Lemma 3, c and p have a common left divisor not a unit. Hence by Theorem 2 they have a greatest common left divisor π which is not a unit, π being uniquely determined up to a unit right factor. If p were the product of π by a unit, p would divide c and hence divide each of its co-ordinates, contrary to the definition of c. Hence $p=\pi d$, where neither π nor d is a unit, whence $p=N(\pi)=N(d)$, so that π is a prime quaternion by Lemma 6.

Write $c=\pi c_1$. Then $N(c_1)=N(c)/p=ql\ldots\ldots$ As before, c_1 and q have a greatest common left divisor κ which is determined uniquely up to a unit right factor, while κ is a prime quaternion whose norm is q. Write $c_1=\kappa c_2$ and proceed with c_2 and l as before. Hence $c=\pi\kappa\lambda\ldots\ldots$

* But each prime factor of the integer m can usually be expressed in many ways as a product of two conjugate prime quaternions.

Let $c=\pi_1\kappa_1\lambda_1 \ldots$. be any factorization of c into prime quaternions π_1, κ_1, ... of norms p, q, ... , respectively. Since $p=\pi_1\pi_1'$ and since c is not divisible by the integer p, π_1 is a greatest common left divisor of c and p. Hence $\pi_1=\pi u$, where u is a unit. Now $c=\pi u\kappa_1$ . . . . and $c=\pi c_1$ imply $c_1=u\kappa_1\lambda_1$. . . . . Also,

$$q=N(\kappa_1)=N(u\kappa_1)=u\kappa_1\kappa_1'u'.$$

Hence $u\kappa_1$ is a greatest common left divisor of c_1 and q, and hence is equal to κu_1, where u_1 is a unit. Thus $\kappa_1=u'\kappa u_1$.

The two expressions for c_1 imply $c_2=u_1\lambda_1$. . . . . This with $l=N(u_1\lambda_1)$ shows that $u_1\lambda_1$ is a greatest common left divisor of c_2 and l, and hence is equal to λu_2, where u_2 is a unit. Thus

$$\pi_1=\pi u, \qquad \kappa_1=u'\kappa u_1, \qquad \lambda_1=u_1'\lambda u_2, \ldots .,$$

where u, u_1, u_2, ... are units and u', u_1', ... are their conjugates as well as reciprocals.

92. Outline of the general theory. First, let A be a rational algebra which is not semi-simple and has a modulus. Then $A=S+N$, where N is the maximal nilpotent invariant sub-algebra of A, and S is a semi-simple sub-algebra of A. It will be proved in §§ 99–104 that the arithmetic of A is associated with that of S. This theorem was illustrated by an example in § 89.

Second, let S be a semi-simple rational algebra and hence a direct sum of simple algebras S_i. By § 93 the arithmetic of S is known completely when we know the arithmetic of each S_i. We shall prove in § 95 the important theorem that for a semi-simple algebra (and no other algebra) of order n each set of integral elements of

order n has a basis, so that the new definition of integral elements essentially coincides with the definitions by Hurwitz and Du Pasquier for the case of semi-simple algebras and only in that case.

Third, let A be a rational simple algebra and hence a direct product of a simple matric algebra and a division algebra D. Then (§ 97) the integral elements of A are known when those of D are known, and conversely. The arithmetic of A is treated in § 98 for several algebras D by generalizing the classic theory of matrices whose elements are integers.

In brief, the problem of arithmetics of all algebras reduces to the case of simple algebras and finally in large measure to the case of division algebras.

93. Arithmetic of a direct sum. Let the rational algebra A having a modulus α be a direct sum of two algebras B and C, called component algebras of A. As proved in § 21, B and C have moduli β and γ whose sum is α.

THEOREM 1. *The first components of the elements of any (maximal) set of integral elements, with properties* R, C, U *of* § 87, *of a direct sum* $B \oplus C$ *constitute a (maximal) set of integral elements of the first component algebra* B, *and similarly for the second components. Conversely, given a (maximal) set* $[b]$ *of integral elements* b *of a rational algebra* B *and a (maximal) set* $[c]$ *of integral elements* c *of another rational algebra* C, *such that* B *and* C *have moduli* β *and* γ *and have* a direct sum, then if we add every* b *to every* c *we obtain sums forming a (maximal) set of integral elements of the direct sum* $B \oplus C$.

* We can always replace B and C by equivalent algebras which have a direct sum (§ 13).

i) Let $[a]$ be any set of integral elements $a=b+c$, $a'=b'+c'$, ... of $A=B\oplus C$, having properties R, C, U, where b, b', ... are in B, and c, c', ... are in C. By the closure property C, $a\pm a'=(b\pm b')+(c\pm c')$ and $aa'=bb'+cc'$ are in $[a]$. Hence the first components b, b', ... form a set $[b]$ having the closure property C. Since the modulus $\alpha=\beta+\gamma$ of A is in $[a]$ by property U, the set $[b]$ contains the modulus β of B.

By property R, for every element a of $[a]$ the coefficients of the rank function $R(\omega)$ of A are integers. By § 72, $R(\omega)$ is the product of the rank functions $R_1(\omega)$ and $R_2(\omega)$ of B and C. By § 83 the $R_i(\omega)$ have integral coefficients, when $R(\omega)$ has integral coefficients. Hence for every element of $[b]$, the coefficients of $R_1(\omega)$ are integers.

This proves the first half of the theorem when both words maximal are omitted. It is proved in (iii) when those words are retained.

ii) Conversely, let $[b]$ and $[c]$ be any sets of integral elements of B and C, respectively. Then all sums $a=b+c$ form a set $[a]$ containing the modulus $\beta+\gamma$ of $A=B\oplus C$, having the closure property C, as well as property R, since for any b and any c in those sets the rank functions of B and C have integral coefficients, whence their product (the rank function of A) has integral coefficients for any a of $[a]$.

Next, let $[b]$ and $[c]$ be maximal sets of B and C, respectively. Then, if the above $[a]$ were not a maximal set of A, it would be contained in a larger set $[a']$ of A. By (i), the first components b' of the $a'=b'+c'$ form a set $[b']$ of elements of B having properties R, C, U, and likewise for the second components c'. Either $[b']$ is

larger than $[b]$ and contains it, or else $[c']$ is larger than $[c]$, contrary to hypothesis.

This proves the second half of the theorem.

iii) Let $[a]$ of case (i) be a maximal set of A. Then if $[b]$ were contained in a larger set $[b']$ of integral elements of B, case (ii) shows that $[b']$ and $[c]$ would determine a set $[a']$ of elements $a'=b'+c$ of A which have properties R, C, U, such that $[a']$ contains the smaller set $[a]$, whereas $[a]$ is a maximal by hypothesis. This completes the proof of the first half of the theorem.

THEOREM 2. *If the element $a=b+c$ of a set $[a]$ of integral elements of $A=B\oplus C$ is a unit, then b and c are units of B and C, respectively, and conversely.*

For, there exists an element $a'=b'+c'$ of $[a]$ such that $aa'=\alpha=\beta+\gamma$, whence $bb'=\beta$, $cc'=\gamma$.

An integral element not a unit is called a *prime* if it admits only such representations as a product of two integral elements of the same algebra in which one of them is a unit.

THEOREM 3. *If the integral elements of determinant $\neq 0$ of the component algebras B and C possess factorization into primes in a single way apart from unit factors, the same is true of the integral elements of determinant $\neq 0$ of $B\oplus C$.*

For example, consider the direct sum

$$(e_1)\oplus(e_2)\oplus(e_3): \qquad e_i^2=e_i, \qquad e_ie_j=0 \qquad (j\neq i).$$

The rank equation of $x=\Sigma\xi_ie_i$ is $\Pi(\omega-\xi_i)=0$. Hence the integral elements x are those having integral coordinates ξ_i. The latter are all $\geqq 0$ in the product of x by a suitably chosen one of the units $\pm e_1\pm e_2\pm e_3$. We may therefore restrict attention to integral elements

x of determinant $\xi_1\xi_2\xi_3 \neq 0$ and having positive co-ordinates. Denote x by (ξ_1, ξ_2, ξ_3). Then $xy = (\xi_1\eta_1, \xi_2\eta_2, \xi_3\eta_3)$. Since

$$(\alpha, \beta, \gamma\delta) = (\alpha, \beta, \gamma)(1, 1, \delta), \quad (\alpha, \beta, \gamma) = (\alpha, \beta, 1)(1, 1, \gamma),$$

one of the co-ordinates of a prime element is a prime number and the remaining two are unity, and conversely every such element is prime. Hence if the α_i, β_j, γ_k are all prime numbers, we have the following unique factorization into prime elements:

$$(\Pi\alpha_i, \Pi\beta_j, \Pi\gamma_k) = \Pi(\alpha_i, 1, 1) \cdot \Pi(1, \beta_j, 1) \cdot \Pi(1, 1, \gamma_k).$$

94. Sets of order n. Let S be a set of elements of a rational algebra A of order n having a modulus, such that S has properties C and U and is of order n. Then S contains n linearly independent elements $v_1, \ldots, v_n$, which may therefore be taken as the basal units of A. By property U the modulus of A belongs to S. Without loss of generality we may evidently assume that v_1 is the modulus. Let therefore

$$v_1v_j = v_j, \quad v_iv_1 = v_i, \quad v_iv_j = \sum_{k=1}^{n} \gamma_{ijk}v_k \quad (i, j = 2, \ldots, n).$$

The γ's are rational numbers. Bring the fractions γ to a common denominator δ and write $\gamma_{ijk} = \nu_{ijk}/\delta$, where δ and the ν are all integers. By property C, the set S contains $u_1 = v_1$, $u_i = \delta v_i (i > 1)$. We have

$$u_1u_j = v_1\delta v_j = \delta v_j = u_j, \qquad u_iu_1 = \delta v_iv_1 = \delta v_i = u_i,$$

$$u_iu_j = \delta^2\left(\gamma_{iji}v_1 + \sum_{k=2}^{n} \gamma_{ijk}v_k\right) = \delta\nu_{iji}u_1 + \sum_{k=2}^{n} \nu_{ijk}u_k,$$

for $i>1$, $j>1$. The constants of multiplication of $u_1, \ldots, u_n$ are all integers.

THEOREM. *If a set S of elements of a rational algebra A of order n having a modulus has properties C and U and is itself of order n, we can choose basal units $u_1, \ldots, u_n$ of A belonging to S such that the constants of multiplication are all integers and u_1 is the modulus.*

95. Existence of a basis for the integral elements of any rational semi-simple algebra A. Let A be of order n and S be any set of elements having properties R, C, U, and order n. By § 94, we can choose basal units $u_1, \ldots, u_n$ of A which belong to S such that u_1 is the modulus and such that the γ's in

$$u_i u_j = \sum_{k=1}^{n} \gamma_{ijk} u_k \qquad (i, j = 1, \ldots, n) \tag{9}$$

are all integers. Let $x = \Sigma \xi_s u_s$ be any element of S. By property C, S contains xu_j. By (9),

$$xu_j = \sum_{i=1}^{n} \rho_{ij} u_i, \qquad \rho_{ij} \equiv \sum_{s=1}^{n} \xi_s \gamma_{sji}.$$

The first characteristic matrix of x is obtained by subtracting ω from each diagonal element of matrix (ρ_{ij}). Apart from sign, the coefficient of ω^{n-1} in the first characteristic equation of x is therefore

$$\sum_{k=1}^{n} \rho_{kk} = \sum_{i,k=1}^{n} \xi_i \gamma_{iik}.$$

Apart from sign, the coefficient c_j of ω^{n-1} in the first characteristic equation of the element xu_j is obtained from the preceding sum by replacing ξ_i by ρ_{ij} and hence is

$$(10) \qquad \sum_{i,\,k,\,s=1}^{n} \xi_s \gamma_{sji}\gamma_{ikk} = c_j \qquad (j=1, \ldots, n).$$

By § 70 the distinct irreducible factors of the characteristic determinant $\delta(\omega)$ of any element X coincide with those of $R(\omega)$, where $R(\omega)=0$ is the rank equation of X. When X is in S, property R shows that the coefficients of $R(\omega)$ are integers, that of the highest power of ω being 1. Hence, by Gauss's lemma in § 83, the same is true of each factor and hence of the product $\delta(\omega)$ of powers of such factors. This proves that each c_j in (10) is an integer.

Let d denote the determinant of the coefficients of $\xi_1, \ldots, \xi_n$ in the n equations (10). Thus $d\xi_s = d_s$, where d_s is the determinant obtained from d by replacing the elements of the sth column by the constant terms $c_1, \ldots, c_n$. Inserting the value d_s/d of ξ_s in $x=\Sigma\xi_s u_s$, we get

$$(11) \qquad x = d^{-1}\Sigma d_s u_s .$$

The elements of d are the sums (27) in § 66, where it was proved that $d \neq 0$ if and only if A is semi-simple.

Since the γ's and the c_j are all integers, d and the d_s are all integers. Hence every element x of S is of the form (11), where the integer d is independent of the particular x, being a function of the γ's alone. The proof in § 86 shows the existence of a basis $\omega_1, \ldots, \omega_n$

of S such that the elements of S coincide with the linear homogeneous functions of the ω's with integral coefficients.

THEOREM. *Let A be any rational semi-simple algebra of order n having a modulus. Let S be any set of elements of A having properties* R, C, U *and of order* n. Then S has a basis $\omega_1, \ldots, \omega_n$, where ω_1 is the modulus.*

But if a rational algebra A is not semi-simple, no maximal set of its elements having properties R, C, U has a basis. For, some of the basal units of A may be taken to be properly nilpotent and we shall find in § 104 that the co-ordinates of those units are arbitrary rational numbers in the general element of a maximal set, so that there is evidently no basis (see the example in § 89).

96. A converse of the theorem above is the case $m=n$ of the

THEOREM. *If for any rational algebra A of order n a set S of elements has the closure property* C *and the property* B_m *of possessing a basis composed of m independent elements, then S has property* R.

First, let $m=n$. Then we may take the elements $u_1, \ldots, u_n$ of the basis of S as new basal units of the algebra. By property C, $u_i u_j$ belongs to S. By property B_n, $u_i u_j$ is equal to a linear function (9) of $u_1, \ldots, u_n$ with integral coefficients γ_{ijk}. Also the co-ordinates of any element $x=\Sigma\xi_i u_i$ of S are integers by property B_n.

* The theorem may fail for sets of order $<n$. Start with a rational algebra Σ having properly nilpotent elements. By § 58, Σ is a subalgebra of a simple matric algebra A. By the text below the theorem, the integral elements of Σ have no basis. The set S of those elements has properties C and U and also R for A by the second case of the proof in § 96.

Hence the characteristic equation $\delta(\omega)=0$ of x has integral coefficients. The same is true of its divisor the rank function by Gauss's lemma (§ 83). Hence S has property R.

Second, let $m<n$. By property C, the elements forming the basis of S are basal units of a rational subalgebra Σ of order m of A. By the first case, S has property R for Σ, so that the rank equation $\rho(\omega)=0$ for Σ has integral coefficients when x is in S. Since $\rho=0$ is invariant under transformation of the units (§ 73) and since S has the same order m as Σ, $\rho=0$ is the minimum equation of the general element x of S. By §§ 67, 68, the first characteristic determinant $\delta(\omega)$ of x for A divides a power of $\rho(\omega)$ and hence has integral coefficients when x is in S. For any x in A, $\delta(\omega)$ is divisible by the rank function $R(\omega)$ of x for A by § 69. Hence for x in S, $R(\omega)$ has integral coefficients by § 83. Thus S has property R for A.

Hence any set of integral elements of a rational algebra A according to the definition of either Hurwitz or Du Pasquier (§ 90) is a set of integral elements under the new definition. Only in the case of a semi-simple algebra A of order n is it true conversely that a set of integral elements of order* n having the properties R, C, U required by the new definition has the property B of possessing a finite basis and hence is a set of integral

* Assumed explicitly by Hurwitz and implicitly by Du Pasquier for the only algebra of which he gave details of finding maximal sets. It might be desirable to add to the new list of postulates for a maximal set of integral elements the assumption (if it be not redundant) that the set shall have the same order as the algebra. Only such sets are treated in § 97. The inclusion of this further assumption would not alter any of the discussions of the entire chapter.

elements according to Du Pasquier's definition, and has a properly chosen set of n basal units and hence has the further property U′ required by Hurwitz.

97. Integral elements of any simple algebra. The theory of arithmetics of semi-simple algebras was reduced to that of simple algebras in § 93. By § 51 a rational simple algebra is the direct product P of a rational division sub-algebra D and a rational simple matric sub-algebra M with n^2 basal units e_{ij} each commutative with every element of D. Furthermore, the modulus Σe_{ii} of M coincides with the moduli of D and P.

Each element p of P may be expressed in the form

$$p = \sum_{i,j=1}^{n} d_{ij} e_{ij}, \tag{12}$$

where the d_{ij} are elements of D. We may express p as the matrix (d_{ij}), a notation to be used in our study (§ 98) of the arithmetic of P. It is desirable that the matrices which are to be called integral shall include the matrices whose elements are all integers, and hence include the basal units* e_{ij}.

If D is of order δ, P is of order δn^2.

THEOREM. *If* Π *is a (maximal) set of elements* (12) *of* P *having properties* R *and* C, *and containing all the matric units* e_{ij} *and having the same order* δn^2 *as* P, *then the* d_{ij} *range independently over a (maximal) set* S *of elements of* D *having properties* R, C, U *and having the same order* δ *as* D, *and conversely.*

* If it were desired to omit this assumption in the definition of a set Π of integral elements of P, we would start with a basis of Π (§ 95). See the concluding remark of § 97.

i) Let Π be a set of elements (12) having properties R and C, and containing every e_{ij} and hence the common modulus Σe_{ii} of M, P, and D. Then Π contains

$$e_{qr}pe_{sq}=d_{rs}e_{qq}\,.$$

Summing for $q=1, \ldots, n$, we see that d_{rs} is in Π. Property R of Π shows that, if in the rank equation of the general element $\Sigma\xi_i u_i$ of P we replace the ξ_i by the co-ordinates of d_{rs}, we obtain an equation $\lambda(\omega)=0$ satisfied by d_{rs} and having integral coefficients and leading coefficient unity.

Let $f(\omega)=0$ be the equation of least degree satisfied by d_{rs} having rational coefficients and leading coefficient unity. It is irreducible in the field R of rational numbers since a product of two elements of a division algebra is zero only when one of them is zero (§ 43, Theorem 4). Then $\lambda(\omega)$ is divisible by $f(\omega)$ since otherwise the remainder from the division would vanish for $\omega=d_{rs}$ and yet be of smaller degree than $f(\omega)$. Hence by Gauss's lemma (§ 83), $f(\omega)$ has integral coefficients.

Let $R(\omega)=0$ be the rank equation of the general element x of D and let it become $\phi(\omega)=0$ for $x=d_{rs}$. By § 70, the distinct irreducible factors of $R(\omega)$ coincide with those of the first characteristic determinant of x. Hence the distinct roots of $\phi(\omega)=0$ are the same as those of the first characteristic equation $\delta(\omega)=0$ of d_{rs}. The same is true of $f(\omega)=0$ and $\delta(\omega)=0$ by § 68. As above (or by Theorem 7 of § 84), ϕ is exactly divisible by f and the quotient is either a constant or is divisible by f, etc. Thus ϕ is a power of f and hence has integral coefficients. This proves that the set S_{rs} composed of

the coefficients of e_{rs} in the various elements (12) of Π is a set of elements d_{rs} of D having property R.

Further, S_{rs} evidently has property U since $1 \cdot e_{rs}$ is in Π. It also has the closure property C. For, if d'_{rs} be the coefficient of e_{rs} in another element (12) of Π, then as above d'_{rs} is in Π. Also the products of d_{rs} and d'_{rs} by e_{rs} are in Π. By the closure property C for Π,

$$(d_{rs}+d'_{rs})e_{rs}, \qquad d_{rs} \cdot d'_{rs}e_{rs}$$

are in Π, whence the sum and product of the d_{rs}'s is in S_{rs}.

Next, if d_{rs} is in S_{rs}, its product by e_{ij} is in Π, whence d_{rs} is in S_{ij}. Hence the n^2 sets S_{rs} $(r, s=1, \ldots, n)$ are identical and may be designated by S. Hence Π is composed of the $\Sigma d_{ij}e_{ij}$ in which the d_{ij} range independently over S.

This proves the first part of the theorem with both words maximal omitted. When they are retained proof is made in (iii).

ii) Conversely, let S be any set of elements of D having properties R, C, U and having the same order δ as D. By § 95, S has a basis $\omega_1, \ldots, \omega_\delta$, where ω_1 is the modulus. Let Π be the set of all $\Sigma d_{ij}e_{ij}$ in which the d_{ij} range independently over S. Then Π has the basis $\omega_k e_{ij}$ $(k=1, \ldots, \delta;\ i, j=1, \ldots, n)$. Also, Π has property C since S does. By § 96, Π has property R. This proves the converse theorem with both words maximal omitted.

Next, let S' be a maximal of the sets S. Then the corresponding Π' is a maximal of the sets Π having the properties assumed in the theorem. For, if Π_1 is such a set which contains Π' and is larger than Π', the set S_1

which corresponds to Π_1 as in (i) is larger than S', contains S', and is one of the sets S, whereas S' is a maximal by hypothesis. This completes the proof of the converse.

iii) Let Π^* be a maximal of the sets Π; then its S^* is a maximal of the sets S having properties R, C, U and having the same order as D. For, if S^* is contained in a larger S, the corresponding Π in (ii) is larger than Π^*, whereas the latter is a maximal. This completes the proof of the first part of the theorem.

COROLLARY. *We know the integral elements of any simple algebra $D\times M$ if we know those of the division algebra D.*

For the case in which D is of order 1, our theorem shows that the set of all matrices whose elements are integers is a maximal of all sets of matrices with rational elements having properties R and C and containing the n^2 units e_{ij}. But if we do not require the presence of the e_{ij}, we find an infinitude of maximal sets. For, any set of matrices with rational elements having properties R, C, U (and M) is transformed into another such set by any matrix with rational elements of determinant $\neq 0$.

98. Arithmetics of certain simple algebras. By § 97, the integral elements of a rational simple algebra $D\times M$ are the n-rowed square matrices $d=(d_{ij})$ in which the d_{ij} range independently over a maximal set S of elements of the rational division algebra D having properties R, C, U.

The product dd' of d by a second such matrix (d'_{ij}) is defined as in § 3 to be the matrix d'' in which the element in the ith row and jth column is

$$d''_{ij}=d_{i1}d'_{1j}+\ \ldots\ .\ +d_{ik}d'_{kj}+\ \ldots\ .\ ,$$

with attention to the order of multiplication. Hence each d''_{ij} is in S.

The constant term of the rank equation of the general element x of D is called the *norm* of x and denoted by $N(x)$. It is a divisor of the first determinant $\Delta(x)$ of x (§ 69). If $x \neq 0$, x has an inverse y in D by the definition of D. By § 58, $\Delta(x)\Delta(y) = 1$, whence $\Delta(x) \neq 0$, $N(x) \neq 0$. Hence $N(x) = 0$ implies $x = 0$.

We shall restrict our attention to maximal sets S of elements of rational division algebras D which possess the following further property:

P. If a and $b (b \neq 0)$ are any two elements of S, there exist elements q, c, Q, C of S such that

$$a = qb + c, \qquad a = bQ + C,$$

where the norms of the remainders c and C are numerically less than the norm of the divisor b.

Evidently property P holds for the important case in which D is of order 1 when the elements of D may be taken to be the rational numbers, so that the elements of S are integers, each being its own norm. Then the following investigation becomes a study of the arithmetic of matrices whose elements are all integers.

Property P was seen in Lemma 2 of § 91 to hold when D is the algebra of rational quaternions. It will be seen in § 105 to hold also for two division algebras which are direct generalizations of the algebra of quaternions.

Two matrices d and d' with elements in S shall be called *equivalent* if and only if $d' = pdq$, where p and q

are products of matrices of the types next displayed for the typical case $n=2$:

$$(13)\quad a_k=\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix},\quad b_k=\begin{pmatrix}1 & 0\\ k & 1\end{pmatrix},\quad c=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\quad e_u=\begin{pmatrix}u & 0\\ 0 & 1\end{pmatrix},$$

where k is any element of S and u is any unit (§ 88) of S. For any n, the types are defined as follows. For each pair of distinct positive integers i and j not exceeding n, we employ a matrix derived from the identity matrix I by replacing the element 0 in the ith row and jth column by k; for $n=2$, it is a_k when $i=1, j=2$, and is b_k when $i=2, j=1$. We employ also a matrix (which is c for $n=2, i=1, j=2$) derived from I by replacing the four elements of

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

which occur at the intersections of the ith and jth rows with the ith and jth columns by the corresponding elements of c. Finally, we employ e_u which is derived from I by replacing the element 1 in the first row and column by u.

The matrices (13) and hence also p and q are units since

$$a_ka_{-k}=I,\qquad b_kb_{-k}=I,\qquad c^2=I,\qquad e_ue_v=I(uv=1).$$

The product a_kd may be obtained from d by adding to the elements of the first row the products of k (as left factor) into the corresponding elements of the second row. The product da_k may be obtained from d by adding to the elements of the second column the products of the corresponding elements of the first column into k

(as right factor). To find $b_k d$ and $d b_k$ we have only to interchange the words first and second in what precedes.

The product cd (or dc) may be obtained from d by interchanging the two rows (or columns) of d.

The product $e_u d$ may be obtained from d by inserting the factor u before each element of the first row of d.

The product de_u may be obtained from d by inserting the factor u after each element of the first column of d.

Hence for any n, matrix d is equivalent to those and only those matrices which may be derived from it by any succession of the following *elementary transformations:*

i) The addition to the elements of any row of the products of any element k of the set S into the corresponding elements of another row, k being used as a left factor.

ii) The addition to the elements of any column of the products of the corresponding elements of another column into any element k of S, k being used as a right factor.

iii) The interchange of any two rows or of two columns.

iv) The insertion of the same unit factor before each element of any row.

v) The insertion of the same unit factor after each element of any column.

We shall call the element d_{11} of matrix d its *first* element. If $d \neq 0$ there exists by (iii) an equivalent matrix whose first element is not zero.

LEMMA 1. *If the first element of a matrix d is not zero and is a left divisor of every element of the first row and*

is a right divisor of every element of the first column, then d is equivalent to a matrix having the same first element and whose further elements in the first row and first column are all zero.

For, if $d_{1i}=d_{11}q_i$, we apply the transformation (ii) which adds to the elements of the ith column the products of those of the first column by $k=-q_i$ and find that the new ith element of the first row is zero. Similarly, if $d_{i1}=Q_id_{11}$, we apply (i) with $k=-Q_i$ and find that the new ith element of the first column is zero.

LEMMA 2. *If the first element d_{11} of a matrix d is not zero and either is not a left divisor of every element of the first row or else is not a right divisor of every element of the first column, then d is equivalent to a matrix for which the first element is not zero and has a norm numerically less than the norm of d_{11}.*

For, if d_{1i} does not have d_{11} as a left divisor, property P shows that we can find elements q and r of S such that $d_{1i}=d_{11}q+r$, where $r\neq 0$ and $N(r)$ is numericaliy $<N(d_{11})$. By (ii) we may add to the elements of the ith column the products of those of the first column by $-q$ and obtain an equivalent matrix having r as the ith element of the first row. By (iii) we obtain an equivalent matrix having r as its first element.

Similarly, if d_{i1} does not have d_{11} as a right divisor, we may write $d_{i1}=Qd_{11}+\rho$, where $\rho\neq 0$, and $N(\rho)$ is numerically $<N(d_{11})$. We then use (i) with $k=-Q$.

Bearing in mind that the norm of any element of S is an integer by property R which is zero only when the element is zero, we see that a finite number of applications of Lemma 2 leads to an equivalent matrix satisfying the hypothesis of Lemma 1. Hence any matrix $d\neq 0$ is

equivalent to a matrix d' whose first element is not zero and whose further elements in the first row and first column are all zero. If the matrix obtained from d' by deleting the first row and first column is not zero, we may apply to it the result just proved for d. Repetitions of this argument show that d is equivalent to a *diagonal* matrix whose elements outside the main diagonal are all zero, while those in the diagonal are $g_{11}, \ldots, g_{nn}$, each of the first r of which are $\neq 0$ and the last $n-r$ are all zero ($1 < r \leqq n$). Denote this matrix by $(g_{11}, \ldots, g_{nn})$ and call r its rank.

If g_{11} is not both a right and a left divisor of all the remaining $g_{jj} \neq 0$, suppose to fix the ideas that g_{11} is not a left divisor of $g_{ii} \neq 0$. We add the elements of the ith row to those of the first row and by (i) obtain an equivalent matrix having g_{ii} as the ith element of the first row. Then by the first part of the proof of Lemma 2 we obtain an equivalent matrix whose first element g'_{11} is not zero and has a norm numerically $< N(g_{11})$. As before we can find an equivalent diagonal matrix whose first element is g'_{11}. After a finite number of repetitions of this process, we reach a diagonal matrix $(h_{11}, \ldots, h_{nn})$ in which h_{11} is not zero and is both a right and a left divisor of each h_{ii}. Treating similarly the matrix $(h_{22}, \ldots, h_{nn})$, we obtain an equivalent matrix $(l_{22}, \ldots, l_{nn})$ in which l_{22} is not zero and is both a right and a left divisor of each l_{ii}. Morevoer, h_{11} is both a right and a left divisor of $l_{22}, \ldots, l_{nn}$ since they are linear combinations of $h_{22}, \ldots, h_{nn}$ with coefficients in S. Proceeding similarly, we obtain the

THEOREM. *Every matrix d of rank $r > 0$, whose elements belong to a maximal set S of elements of a division*

algebra D for which properties R, C, U, P *hold, is equivalent to a diagonal matrix* $(d_1, \ldots, d_r, 0, \ldots, 0)$, *where each* d_i *is both a right and a left divisor of* d_{i+1}, $d_{i+2}, \ldots$. *Here* d_i *may be replaced by* ud_iv, *where* u *and* v *are any units of* S.

The final remark follows from (iv) and (v).

We shall call $(u_1, \ldots, u_n)$ a *unit* if $u_1, \ldots, u_n$ are any units of S. Employing only matrices whose elements are in S, we shall call a matrix d a *prime* matrix if it is not a unit and if it admits only such representations as a product of two matrices in which one of them is a unit.

By definition any matrix equivalent to d is of the form pdq where the matrices p and q are units of the algebra. In other words any matrix d is associated (§ 88) with a diagonal matrix.

First, let S be the set of integers so that the elements of our matrices are integers. Then any matrix d of rank n will be expressible as a product of prime matrices in one and only one way apart from unit factors if the like property is proved for diagonal matrices. The latter is proved essentially* as at the end of § 93. Hence unique factorization into prime matrices holds.

Second, let S be the set of integral quaternions. The uniqueness of factorization of diagonal matrices and hence of any matrices whose elements are integral quaternions is subject to the same limitations as in Theorem 5 of § 91.

* We now need consider $(\alpha, \beta, \gamma\delta)$ only when α divides β and when α and β both divide $\gamma\delta$. For example, if $\gamma = \beta$, we employ

$$(\alpha, \beta, \beta\delta) = (\alpha, \beta, \beta)\ (1, 1, \delta).$$

While we there employed $(\alpha, \beta, 1)$, we would now use the equivalent matrix $(1, \alpha, \beta)$.

99. The fundamental theorem on arithmetics of algebras. The proof (§ 104) for any rational algebra depends upon that for the complex algebra with the same basal units. Hence we shall first deduce from the general theory of algebras a set of normalized basal units of any complex algebra and derive its characteristic determinants by a method far simpler than that employed by Cartan.* Moreover, our notations are more explicit and hence more satisfactory.

It is only incidental to the goal of rational algebras that we find the integral elements of a normalized complex algebra. That result alone would not dispose of the question for all rational algebras since not all types of the latter are rational sub-algebras of complex algebras in canonical forms obtained by applying transformations of units with complex coefficients.

100. Normalized basal units of a nilpotent algebra.

LEMMA. *Any associative algebra A of index α is a sum of α linear sets $B_1, \ldots, B_\alpha$, no two with an element $\neq 0$ in common, such that*

$$(14)\quad B_\rho B_\sigma \leqq B_{\rho+\sigma} + B_{\rho+\sigma+1} + \ldots + B_\alpha \qquad (\rho+\sigma<\alpha),$$

$$(15)\quad B_\rho B_\sigma \leqq B_\alpha \qquad (\rho+\sigma\geqq\alpha).$$

For, we may select in turn linear sets $B_1, B_2, \ldots$ such that

$$A = B_1 + A^2,\ A^2 = B_2 + A^3, \ldots, A^{\alpha-1} = B_{\alpha-1} + A^\alpha,\ A^\alpha = B_\alpha,$$

where $B_i \wedge A^{i+1} = 0$ in $A^i = B_i + A^{i+1}$. Thus $B_i \leqq A^i$. For $i<j\leqq\alpha$,

$$B_j \leqq A^j \leqq A^{i+1}, \qquad B_i \wedge B_j = 0.$$

* *Annales Fac. Sc. Toulouse*, Vol. XII (1898). See the author's *Linear Algebras* (1914), pp. 44–55.

Evidently,

$$A = B_1 + B_2 + \ldots + B_\alpha, \qquad B_p B_q \leqq A^p A^q.$$

Now A^{p+q} is B_α if $p+q \geqq \alpha$; but, for $p+q < \alpha$,

$$A^{p+q} = B_{p+q} + A^{p+q+1} = B_{p+q} + B_{p+q+1} + A^{p+q+2}$$
$$= \ldots = B_{p+q} + \ldots + B_\alpha.$$

We now assume that A is nilpotent and of index α, so that $B_\alpha = 0$. Let $n_1, \ldots, n_{b_1}$ be a basis of B_1, i.e., linearly independent elements of B_1 such that every element of B_1 is a linear combination of them with coefficients in the field F over which A is defined. Let $n_{b_1+1}, \ldots, n_{b_1+b_2}$ be a basis of B_2, etc.

First, let $p \leqq q$ and $p+q < \alpha$. Then in the bases of B_p and B_q, each n has a subscript $\leqq b_1 + \ldots + b_q$. The latter sum is less than the minimum subscript $b_1 + \ldots + b_{p+q-1} + 1$ of an n in B_{p+q}. Hence by (14), *every product $n_i n_j$ is a linear combination with coefficients in F of those n's whose subscripts exceed both i and j.*

The same result holds also if n_i is in B_p and n_j is in B_q, where now $p+q \geqq \alpha$, since $B_p B_q = 0$ by (15), so that $n_i n_j = 0$.

A set of basal units $n_1, n_2, \ldots$ of a nilpotent algebra is called a *normalized* set if it has the property expressed in italics.

101. The two categories of complex algebras. By § 79, every complex algebra A with a modulus e is the sum of its maximal nilpotent invariant sub-algebra N and a semi-simple sub-algebra S, while S is a direct sum of simple matric algebras S_i. Here N must be replaced by 0 if A itself is semi-simple. According as the orders

of the S_i are all 1 or not all 1, A is said to be of the *first* or *second category*, respectively.

This separation of the two cases is nowise necessary in the present theory, but is a convenient one since the notations in the first case are much simpler than in the second case. Although the later treatment of the second case applies to both cases, the prior simple discussion of the first case will greatly clarify that of the second case.

102. Complex algebras A of the first category. We have $A=S+N$, where S is a direct sum of algebras $(e_1), \ldots, (e_h)$ of order 1, and

$$(16) \qquad e_i^2=e_i\,, \qquad e_ie_j=0 (i\neq j), \qquad \Sigma e_i=e\,,$$

e being the modulus of both A and S. Thus

$$N=eNe=\sum_{i,j=1}^{h} e_iNe_j\,.$$

If e_iNe_j is not zero, its elements are all linear combinations of certain of its elements $n_1, n_2, \ldots$, which are linearly independent. Since $n_\rho=e_ixe_j$, where x is in N, we have

$$(17) \quad e_in_\rho=n_\rho\,, \quad e_kn_\rho=0 (k\neq i)\,, \quad n_\rho e_j=n_\rho\,, \quad n_\rho e_t=0 \ (t\neq j)\,,$$

for $k, t=1, \ldots, h$. Any element $n_\rho\neq 0$ which satisfies these conditions (17) is said to have the *character* (i, j). But if $e_iNe_j=0$, N has no elements of character (i, j). Write

$$e_iNe_j=C_{ij}+e_iN^2e_j\,,$$

where the two linear sets on the right have only zero in common. Every element $\neq 0$ of C_{ij} is of character (i, j). Then

$$N^2 = eN^2e = \Sigma e_i N^2 e_j, \qquad N = B_1 + N^2, \qquad B_1 = \Sigma C_{ij},$$

summed for $i, j = 1, \ldots, h$. Hence the elements of B_1 are linear combinations of elements each having a definite character. The same is true of B_2 in $N^2 = B_2 + N^3$, etc. In view also of § 100 we may therefore choose a normalized set of basal units of N each having a definite character.

THEOREM 1. *Any complex algebra A of the first category has a set of basal units $e_1, \ldots, e_h, n_1, \ldots, n_g$, where each n_ρ is nilpotent and has a definite character, while*

$$(18) \quad e_i^2 = e_i, \qquad e_i n_\rho = n_\rho, \qquad n_\rho e_j = n_\rho, \qquad n_\rho n_\sigma = \Sigma \gamma_{\rho\sigma\tau} n_\tau,$$

summed for $\tau = 1, \ldots, g$; $\tau > \rho$, $\tau > \sigma$; such that n_ρ, n_σ, n_τ have the respective characters (i, j), (j, l), (i, l). All further products of two units are zero.

To find the first characteristic determinant $\delta(\omega)$ of the general element $z = x + y$ of A, where

$$x = \xi_1 e_1 + \ldots + \xi_h e_h, \qquad y = \nu_1 n_1 + \ldots + \nu_g n_g,$$

we proceed as in the footnote to § 60. If n_σ is of character $(j, -)$,

$$ze_j = \xi_j e_j + \text{lin. func. of } n_1, \ldots, n_g;$$
$$zn_\sigma = \xi_j n_\sigma + \text{lin. func. of } n_{\sigma+1}, n_{\sigma+2}, \ldots.$$

Transposing the left members after replacing z by ω, we obtain linear equations in the units such that the elements below the main diagonal of the determinant of

the coefficients are all zero, while each diagonal element is a $\xi_j-\omega$. Hence $\delta(\omega)$ is a product of powers of $\xi_j-\omega$ $(j=1, \ldots, h)$ with exponents $\geqq 1$. By § 70, the same is true of the rank function $R(\omega)$, in which the coefficient of the highest power of ω is unity.

We are now in a position to investigate the sets of elements of A with rational co-ordinates which have properties R, C, U of §87. To secure the closure property C, we assume that the γ's in (18) are rational. By property R, each coefficient of $R(\omega)=0$ is an integer. Since its roots ξ_j are all rational, they are integers. The maximal set is composed of all elements z in which the ξ_j are integers, while the ν_j are merely rational. All such z's therefore give the integral elements of A.

We shall prove that $u=1+\Sigma a_\rho n_\rho$ is a unit (§ 88) for all rational values of the a_ρ. First,

$$u(1-a_1n_1)=1-a_1^2n_1^2+l_2=1+a_{12}n_2+l_3\equiv u_2\,,$$

where l_i denotes a linear function of $n_i, n_{i+1}, \ldots$ with rational coefficients. Similarly,

$$u_2(1-a_{12}n_2)=1-a_{12}^2n_2^2+l_3'=1+a_{13}n_3+l_4\,.$$

Proceeding in this manner, we finally reach the product 1. Hence

$$uv=1, \quad v=(1-a_1n_1)(1-a_{12}n_2)(1-a_{13}n_3)\ldots=1+\Sigma b_in_i\,,$$

where the b_i are rational. Hence u and v are units.

If n_ρ is of character (i, j), and $\xi_1, \ldots, \xi_h$ are all $\neq 0$,

$$xu=x+\sum_\rho a_\rho\xi_in_\rho=x+y=z$$

provided $a_\rho = \nu_\rho \xi_i^{-1}$. Multiply by v. Hence $zv = x$. This proves that, if $\Delta(z) \neq 0$, so that each $\xi_i \neq 0$, z is associated with its abridgment x. Recalling the definition of associated arithmetics (§ 88), we have

THEOREM 2. *If the γ's are rational for the algebra $A = S + N$ in Theorem 1, the arithmetic of A is associated with the arithmetic of the sub-algebra S having the basal units $e_1, \ldots, e_h$.*

103. General complex algebra. Any complex algebra A with a modulus e is the sum of its maximal nilpotent invariant sub-algebra N and a semi-simple algebra S which is a direct sum of t simple matric algebras S_i. Then S_i has the basal units $e^i_{\alpha\beta}$ ($\alpha, \beta = 1, \ldots, p_i$), with

$$(19) \quad e^i_{\alpha\beta} e^i_{\beta\gamma} = e^i_{\alpha\gamma}, \qquad e^i_{\alpha\beta} e^i_{\gamma\delta} = 0 (\beta \neq \gamma), \qquad e^i_{\alpha\beta} e^j_{\gamma\delta} = 0 (i \neq j),$$

$$(20) \quad e = \sum_{i,\alpha} e^i_{\alpha\alpha}, \qquad N = eNe = \sum_{i,j,\alpha,\beta} e^i_{\alpha\alpha} N e^j_{\beta\beta}.$$

If ν is an element of N such that

$$n \equiv e^i_{\alpha\alpha} \nu e^j_{\beta\beta} \neq 0,$$

then

$$(21) \quad \begin{cases} e^i_{\alpha\alpha} n = n, & e^k_{\gamma\gamma} n = 0 \quad \text{(unless } k = i, \gamma = \alpha), \\ n e^j_{\beta\beta} = n, & n e^k_{\gamma\gamma} = 0 \quad \text{(unless } k = j, \gamma = \beta), \end{cases}$$

and n is said to have the *character*

$$(22) \quad \begin{pmatrix} i & j \\ \alpha & \beta \end{pmatrix}.$$

Let i and j be fixed integers such that $e^i_{11} \nu e^j_{11}$ is not zero for every ν in N and let $\nu_1, \nu_2, \ldots$ be elements of N such that

$$(23) \qquad \begin{bmatrix} i & j \\ 1 & 1 \end{bmatrix}_\rho \equiv e^i_{11}\nu_\rho e^j_{11} \qquad (\rho = 1, 2, \ldots .)$$

form a complete set of linearly independent elements of N of character

$$(24) \qquad \binom{i \quad j}{1 \quad 1},$$

whence every element of that character is a linear function of the elements (23). By (23),

$$P_\rho = e^i_{\alpha 1}\begin{bmatrix} i & j \\ 1 & 1 \end{bmatrix}_\rho e^j_{1\beta} = e^i_{\alpha\alpha}k_\rho e^j_{\beta\beta} \equiv \begin{bmatrix} i & j \\ \alpha & \beta \end{bmatrix}_\rho, \qquad k_\rho \equiv e^i_{\alpha 1}\nu_\rho e^j_{1\beta},$$

whence P_ρ is of character (22). Since N is invariant in A, k_ρ belongs to N. We shall prove that the P_ρ, with i, j, α, β fixed, form a complete set of linearly independent elements of N of character (22). First, if they were dependent, $\Sigma c_\rho P_\rho = 0$ for complex numbers c_ρ not all zero, we multiply by $e^i_{1\alpha}$ on the left and by $e^j_{\beta 1}$ on the right and get

$$\sum_\rho c_\rho \begin{bmatrix} i & j \\ 1 & 1 \end{bmatrix}_\rho = 0,$$

whence each $c_\rho = 0$, contrary to hypothesis. Hence the number of elements in a complete set of character (22) is not less than the number in a complete set of character (24). To prove the reverse, note that if a set of P_ρ are linearly independent, the corresponding elements (23) will be linearly independent, since we saw how to deduce P_ρ from (23) by multiplying by $e^i_{\alpha 1}$ on the left and by $e^j_{1\beta}$ on the right.

In view of (20), the aggregate of the elements in the complete sets just described for the various values of i, j, α, β gives a set of basal units of N, each having a definite character.

By (19), the product of $e^i_{1\mathrm{I}}\nu_\rho e^j_{1\mathrm{I}}$ by $e^k_{1\mathrm{I}}\nu'_\sigma e'_{1\mathrm{I}}$ is zero if $j \neq k$, while if $j = k$ it is $e^i_{1\mathrm{I}} \cdot \nu_\rho e^j_{1\mathrm{I}}\nu'_\sigma \cdot e'_{1\mathrm{I}}$, which is zero or of character

$$\begin{pmatrix} i & l \\ \mathrm{I} & \mathrm{I} \end{pmatrix}.$$

Hence

$$(25)\quad \begin{bmatrix} i & j \\ \mathrm{I} & \mathrm{I} \end{bmatrix}_\rho \cdot \begin{bmatrix} k & l \\ \mathrm{I} & \mathrm{I} \end{bmatrix}_\sigma = \begin{cases} 0 & (j \neq k), \\ \sum_\tau \gamma^{ij'}_{\rho\sigma\tau} \begin{bmatrix} i & l \\ \mathrm{I} & \mathrm{I} \end{bmatrix}_\tau & (j = k). \end{cases}$$

From this we shall deduce

$$(26)\quad \begin{bmatrix} i & j \\ \alpha & \beta \end{bmatrix}_\rho \cdot \begin{bmatrix} k & l \\ \lambda & \mu \end{bmatrix}_\sigma = \begin{cases} 0 & (j \neq k \text{ or } \beta \neq \lambda), \\ \sum_\tau \gamma^{ij'}_{\rho\sigma\tau} \begin{bmatrix} i & l \\ \alpha & \mu \end{bmatrix}_\tau & (j = k,\ \beta = \lambda). \end{cases}$$

For, the left member denotes the product

$$e^i_{\alpha\mathrm{I}} \begin{bmatrix} i & j \\ \mathrm{I} & \mathrm{I} \end{bmatrix}_\rho e'_{1\beta} \cdot e^k_{\lambda\mathrm{I}} \begin{bmatrix} k & l \\ \mathrm{I} & \mathrm{I} \end{bmatrix}_\sigma e'_{1\mu},$$

which is zero if either $j \neq k$ or $\beta \neq \lambda$. In the remaining case, the product of the juxtaposed e's is $e'_{1\mathrm{I}}$, which produces no effect on (23) when used as a right-hand multiplier. To evaluate our expression, it therefore remains to multiply (25) on the left by $e^i_{\alpha\mathrm{I}}$ and on the right by $e'_{1\mu}$; the result is the sum in (26).

The complete multiplication table of A is given by (19), (26), and

$$(27)\qquad e^{i}_{\alpha\beta}\begin{bmatrix} k & l \\ \lambda & \mu \end{bmatrix}_{\sigma} = \begin{cases} 0 & (i \neq k \text{ or } \beta \neq \lambda), \\ \begin{bmatrix} k & l \\ \alpha & \mu \end{bmatrix}_{\sigma} & (i=k,\ \beta=\lambda), \end{cases}$$

$$(28)\qquad \begin{bmatrix} i & j \\ \alpha & \beta \end{bmatrix}_{\rho} e^{k}_{\gamma\delta} = \begin{cases} 0 & (k \neq j \text{ or } \gamma \neq \beta), \\ \begin{bmatrix} i & j \\ \alpha & \delta \end{bmatrix}_{\rho} & (k=j,\ \gamma=\beta). \end{cases}$$

We arrange our basal units of N in the order n_1, n_2, ... , where n_1, ... , n_{b_1} are those of our units of N which are not in N^2, while n_{b_1+1}, ... , $n_{b_1+b_2}$ are those of N^2 which are not in N^3, etc.

The general element of A is $z=x+y$, where

$$x=\Sigma\xi^{i}_{\alpha\beta}e^{i}_{\alpha\beta}, \qquad y=\Sigma\eta^{ij}_{\alpha,\beta,\rho}\begin{bmatrix} i & j \\ \alpha & \beta \end{bmatrix}_{\rho}.$$

We seek the first characteristic determinant $\delta(\omega)$ of z. First,

$$(29)\qquad ze^{k}_{\gamma\delta}=\sum_{\alpha}\xi^{k}_{\alpha\gamma}e^{k}_{\alpha\delta}+(n_1, n_2, \ldots .),$$

where the final symbol denotes a linear function of n_1, n_2, ... Next, let

$$\begin{bmatrix} k & l \\ \lambda & \mu \end{bmatrix}_{\sigma}=n_t(t\leqq b_1), \qquad \begin{bmatrix} k & l \\ \alpha & \mu \end{bmatrix}_{\sigma}=n_s,$$

so that n_t is in N, but not in N^2. The same is true of n_s and of any basal unit obtained from n_t by varying only λ and μ, as shown by comparing (25) with (26). Hence by (27),

$$(30)\qquad zn_t=\sum_{\alpha}\xi^{k}_{\alpha\lambda}n_s+(n_{b_1+1},\ n_{b_1+2}, \ldots .).$$

For the next step, let

$$\begin{bmatrix} k & l \\ \lambda & \mu \end{bmatrix}_\sigma = n_p \ (b_1 < p \leqq b_1 + b_2), \qquad \begin{bmatrix} k & l \\ a & \mu \end{bmatrix}_\sigma = n_q,$$

so that n_p is in N^2, but not in N^3. The same is true of n_q as before. Hence

$$(31) \qquad z n_p = \sum_a \xi^i_{a\lambda} n_q + (n_{b_1+b_2+1}, \ n_{b_1+b_2+2}, \ \ldots).$$

Replacing z by ω and transposing the left members of (29), (30), (31), ... , we see that the determinant $\delta(\omega)$ of the coefficients of the e's and n's is a product of powers (with exponents $\geqq 1$) of the determinants

$$D_i(\omega) = \begin{vmatrix} \xi^i_{11} - \omega & \xi^i_{12} & \ldots & \xi^i_{1p_i} \\ \ldots & \ldots & \ldots & \ldots \\ \xi^i_{p_i 1} & \xi^i_{p_i 2} & \ldots & \xi^i_{p_i p_i} - \omega \end{vmatrix}.$$

Thus $\delta(\omega)$ is independent of the co-ordinates η of y. The same is therefore true of the rank function $R(\omega)$ which is a divisor of $\delta(\omega)$.

We are now in a position to investigate the sets of elements of A with rational co-ordinates which have properties R, C, U of § 87. To secure the closure property C, we assume that the γ's in (25) are rational. The maximal set of integral elements of A is composed of the $z = x + y$ in which co-ordinates of y are arbitrary rational numbers, while the x's form a maximal set of integral elements of the sub-algebra S.

If the a_ρ are rational, $1 + \Sigma a_\rho n_\rho$ is a unit (§ 102).

If the determinant $\Delta(z) = \delta(0)$ of z is not zero, we can find a unit

$$u=1+\sum_{k,j,\lambda,\beta,\rho} a^{kj}_{\lambda\beta\rho}\begin{bmatrix} k & j \\ \lambda & \beta \end{bmatrix}_\rho,$$

such that $xu=x+y=z$. In fact,

$$xu=x+\Sigma\xi^i_{\alpha\lambda}a^{ij}_{\lambda\beta\rho}\begin{bmatrix} i & j \\ \alpha & \beta \end{bmatrix}_\rho,$$

summed for $\lambda, i, j, \alpha, \beta, \rho$. This sum will be identical with y if

$$\sum_\lambda \xi^i_{\alpha\lambda}a^{ij}_{\lambda\beta\rho}=\eta^{ij}_{\alpha\beta\rho}$$

for all $i, j, \alpha, \beta, \rho$. The determinant of the coefficients of the a's having i, j, β, ρ fixed and $\lambda=1, \ldots, p_i$, is

$$D_i(0)=|\xi^i_{\alpha\lambda}| \qquad (\alpha, \lambda=1, \ldots, p_i),$$

which is zero for no value of i since $\delta(0)$ was shown to be a product of powers (with exponents $\geqq 1$) of the $D_i(0)$. There exists a unit v such that $uv=1$. Hence $zv=x$, so that z is associated with x.

THEOREM. *Any complex algebra $A=S+N$ with a modulus has a set of basal units each with a definite character and having the multiplication table* (19), (26), (27), *and* (28). *If the γ's are rational, the arithmetic of A is associated with the arithmetic of its semi-simple sub-algebra S.*

104. Arithmetic of any rational algebra. Let A be any algebra with a modulus over the field of all rational numbers, such that A is not semi-simple. Let N denote its maximal nilpotent invariant sub-algebra. By § 78, $A=S+N$, where S is a semi-simple sub-algebra.

Let A', S', N' denote the algebras over the field of all complex numbers which have the same basal units as A, S, N, respectively. Then S' is semi-simple and N' is the maximal nilpotent invariant sub-algebra of $A'=S'+N'$ (§ 74). Introduce the basal units of A' which were employed in §§ 102–3. As there proved, the first characteristic determinant and rank function of A' does not involve the co-ordinates of the basal units belonging to N'. Hence the rank equation $R(\omega)=0$ of A does not involve the co-ordinates of the basal units ζ_ρ belonging to N, which are therefore arbitrary rational numbers in any integral element of A. Denote the basal units of S by s_i. Then every element of A is of the form

$$z=x+y, \qquad x=\Sigma X_i s_i, \qquad y=\Sigma Y_\rho \zeta_\rho,$$

where X_i and Y_ρ are rational. Let

$$\Delta(z)\neq 0, \qquad u=1+\Sigma a_\rho \zeta_\rho.$$

Then

$$xu=x+\sum_{i,\rho} X_i a_\rho s_i \zeta_\rho.$$

Since N, of order g, is invariant in A,

$$s_i \zeta_\rho=\sum_{k=1}^{g} \gamma_{i\rho k}\zeta_k,$$

where the γ's are rational. Hence $xu=x+y=z$ if

$$\sum_{i,\rho} \gamma_{i\rho k} X_i a_\rho = Y_k \qquad (k=1, \ldots, g).$$

These g linear equations in g unknowns a_ρ with rational coefficients are consistent and have unique

solutions α_ρ, which are therefore rational. In fact, after introducing the basal units of A' employed in §§ 102–3, we proved that there exists one and only one set of co-ordinates of u such that $xu=z$, so that the same is true when we return to the present basal units.

We can determine rational numbers β_i such that (§ 102, end)

$$uv=1, \qquad v=1+\Sigma\beta_i\zeta_i.$$

Hence u and v are units, and $xu=z$ implies $zv=x$, whence z is associated with its abridgment x if $\Delta(z)\neq 0$.

FUNDAMENTAL THEOREM. *The arithmetic of $A=S+N$ is associated with the arithmetic of its semi-simple sub-algebra S. In other words, we may suppress the properly nilpotent elements of an algebra when studying its arithmetic.*

105. Generalized quaternions. Consider the algebra D whose elements are $X=x+yE$, where x and y range over all complex numbers with rational co-ordinates, such that

$$E^2=-\beta, \qquad Ex=x'E, \tag{32}$$

where $x'=\sigma-\xi i$ is the conjugate of* $x=\sigma+\xi i$. If $-\beta$ is not a sum of two rational squares, D is a division algebra (§ 47, where x, y, γ are now replaced by i, E, $-\beta$, and we have taken $\delta=-1$). We restrict β to integral values.

* Writing $y=\eta+\zeta i$, we see that X is the general element of the algebra (18) of § 10 with $\alpha=1$, $u_1=i$, $u_2=E$, $u_3=iE$, so that D is a generalization of the algebra of quaternions (the case $\beta=1$). As proved there, D is associative. The arithmetic of algebra (18) for any α and β is being studied by other methods by Latimer in his Chicago thesis.

The product of X by $Z=z+wE$ is

$$XZ=xz-\beta yw'+(xw+yz')E, \tag{33}$$

which is an element of D, so that D is an associative algebra. We shall call $\bar{X}=x'-yE$ the *conjugate* of X, and

$$N(X)=X\bar{X}=\bar{X}X=xx'+\beta yy' \tag{34}$$

the *norm* of X. The conjugate of XZ in (33) is seen to be equal to the product $\bar{Z}\bar{X}$ of the conjugates of the factors taken in reverse order. Hence

$$N(XZ)=XZ\bar{Z}\bar{X}=X\bar{X}Z\bar{Z}=N(X)\cdot N(Z), \tag{35}$$

since $Z\bar{Z}$ is a rational number and hence is commutative with $\bar{X}$. Note that X and $\bar{X}$ are the roots of

$$\omega^2-2\sigma\omega+N(X)=0 \qquad (x=\sigma+\xi i). \tag{36}$$

Consider the set I of all elements $X=x+yE$ in which x and y are complex integers (i.e., complex numbers with integral co-ordinates). Then the coefficients of the rank equation (36) are integers. In view also of (33), we see that the set I has the closure property C.

We shall now determine every set S of elements X of D which has properties R and C and contains I. For the moment give X, x, y the foregoing notations and call σ the rational part of X. Since 1, E, and Ei belong to I and hence to S, the closure property C shows that S contains X, Xi, $XE=-\beta y+xE$, and XEi, whose rational parts are evidently σ, $-\xi$, $-\beta\eta$, $\beta\zeta$, respectively. The negatives of their doubles are therefore coefficients of the rank equations of X, Xi, etc., and hence are integers by property R. In other words, $2x$ and $2\beta y$ are complex integers, say u and w. Then

$$X=\tfrac{1}{2}\left(u+\frac{1}{\beta}wE\right), \qquad N(X)=\tfrac{1}{4}\left(uu'+\frac{1}{\beta}ww'\right).$$

By (36) and property R, $N(X)$ must be an integer, so that ww' must be divisible by β.

If c is a complex integer $\neq 0$, the introduction of $c^{-1}E$ as a new unit in place of E has the effect of dividing β by cc'. Hence we may assume that β is not divisible by a sum of two integral squares. It is known that every prime of the form $4n+1$ and every product of such primes is a sum of two integral squares. Also, $2=1^2+1^2$. Hence we may assume that $\pm\beta$ is either unity or a product of distinct primes of the form $4n+3$.

LEMMA *If such a β divides $\gamma^2+\delta^2$, where γ and δ are integers, then β divides both γ and δ.*

For, if $p=4n+3$ is a prime factor of β and hence of $\gamma^2+\delta^2$, either p divides γ and hence also δ, or we can find (§ 110, end) an integer ϵ such that $\gamma\epsilon\equiv 1 \pmod{p}$. Then

$$0\equiv(\gamma^2+\delta^2)\epsilon^2\equiv 1+(\delta\epsilon)^2 \pmod{p},$$

whereas -1 is known to be not congruent to a square modulo $p=4n+3$. Hence p divides γ and δ. Thus $\beta=p\beta_1$ divides p^2s, where

$$s=(\gamma/p)^2+(\delta/p)^2.$$

Since β has no square factor, β_1 divides s. As before, any prime factor q of β_1 divides both γ/p and δ/p. Proceeding similarly, we conclude that $\beta=pq\ldots.$ divides both γ and δ.

We proved above that β must divide $ww'=\gamma^2+\delta^2$, if we write $w=\gamma+\delta i$. Hence β divides γ and δ and hence

also w. Write $w=\beta v$. Thus every element of S is of the form $X=\frac{1}{2}(u+vE)$, where u and v are complex integers. Then

$$N(X)=\tfrac{1}{4}(uu'+\beta vv') \tag{37}$$

must be an integer.

First, let $\beta\equiv 1 \pmod 4$. By (37), $uu'+vv'$, which is a sum of four integral squares, must be divisible by 4. They must all be even or all odd since the square of an even or odd integer has the remainder 0 or 1, respectively, when divided by 4. The maximal set S is therefore composed of all elements $\frac{1}{2}(u+vE)$ in which the four co-ordinates of the complex integers u and v are either all even or all odd integers. If in the latter case we subtract

$$G=\tfrac{1}{2}(1+i+E+iE), \tag{38}$$

we obtain a linear combination of $1, i, E, iE$ with integral coefficients. Since $iE=2G-1-i-E$, the set S has the basis $1, i, E, G$. Since $E=(1-i)G-1$, S is composed of the elements $x+yG$, where x and y are complex integers. This set S is closed under multiplication since

$$Gi=-1+i-iG, \qquad G^2=G-\tfrac{1}{2}(1+\beta).$$

This completes the proof of the first part of the theorem below.

Second, let $\beta\equiv 3 \pmod 4$. By (37), the integers uu' and vv' must be congruent modulo 4. Write $u=\kappa+\lambda i$, $v=\mu+\nu i$. Then $\kappa^2+\lambda^2\equiv\mu^2+\nu^2 \pmod 4$. Hence the values of $\kappa, \lambda, \mu, \nu$ are congruent modulo 2 to those in one of the six sets

$$(0000),\ (0110),\ (0101),\ (1010),\ (1001),\ (1111). \tag{39}$$

For the first of these sets, $X=\frac{1}{2}(u+vE)$ is of the form $x+yE$, where x and y are complex integers, and hence belongs to the set I of all such elements. If from the half of any complex integer we subtract a suitably chosen complex integer x, we obtain $\frac{1}{2}u$, where $u=\kappa+\lambda\imath$, $\kappa=0$ or 1, $\lambda=0$ or 1. Hence any element of S is the sum of a suitably chosen element $x+yE$ of I and an element $H=\frac{1}{2}(u+vE)$ for which $(\kappa, \lambda, \mu, \nu)$ is identical with one of the sets (39) and not merely congruent to it. Hence S is derived from I by annexing one or more of the elements $H_2, \ldots, H_6$ defined by the second, . . . , sixth set (39), respectively.

Let S_1 be the set obtained by annexing either of

$$H_2=\tfrac{1}{2}(i+E), \qquad H_5=\tfrac{1}{2}(1+iE) \tag{40}$$

to I. It contains both of them since

$$H_2E=H_5-\tfrac{1}{2}(1+\beta), \qquad H_5E=H_2-\tfrac{1}{2}i(1+\beta),$$

while $1+\beta$ is an even integer.

Let S_2 be the set obtained by annexing either of

$$H_3=\tfrac{1}{2}i(1+E), \qquad H_4=\tfrac{1}{2}(1+E) \tag{41}$$

to I. It contains both of them since

$$iE\cdot H_3=H_4-\tfrac{1}{2}(1+\beta), \qquad iE\cdot H_4=H_3-\tfrac{1}{2}i(1+\beta).$$

If we annex all of the elements (40) and (41), we obtain a set containing $H_4+H_2-E=\frac{1}{2}(1+i)$, whose norm is $\frac{1}{2}$, so that the set does not have properties R and C.

If to I we annex $H_6=G$, given by (38), we obtain a set containing $G=H_2+H_5=H_3+H_4$, so that the set is a sub-set of both S_1 and S_2.

Hence the only maximal sets containing I are S_1 and S_2. In view of their origin they have properties R and U. It remains to verify that they have the closure property C.

Note that S_1 has the basis 1, i, H_2, H_5 since from the first two and the doubles of the last two we deduce E and iE and hence the basis of I. Since $H_5 = iH_2 + 1$, the elements of S_1 are all of the form $x + yH_2$, where x and y are complex integers. Thus S_1 is closed under multiplication since

$$H_2 i = -1 - iH_2, \qquad H_2^2 = -\tfrac{1}{4}(1+\beta).$$

Similarly, S_2 has the basis 1, i, $H_3 = iH_4$, H_4, and is closed under multiplication since

$$H_4 i = i - iH_4, \qquad H_4^2 = H_4 - \tfrac{1}{4}(1+\beta).$$

THEOREM. *Let D be the algebra composed of the elements $x+yE$, where x and y range over all complex numbers with rational co-ordinates, while $E^2 = -\beta$, $Ex = x'E$, and β is an integer. Without loss of generality we may take β to be ± 1 or a product of distinct primes of the form $4n+3$ or the negative of such a product. Then every maximal set of elements having properties* R *and* C, *and containing the basal units* 1, i, E, iE, *is formed of all the elements $x+yB$, where x and y range over all complex integers, while B is given by* (38) *if $\beta \equiv 1 \pmod 4$, but B is either H_2 or H_4 in* (40) *or* (41) *if $\beta \equiv 3 \pmod 4$. Hence in the latter case, D has two such maximal sets. Except for $\beta = -1$, D is a division algebra.*

It remains only to prove the final remark in the theorem. As noted above, D is a division algebra if $-\beta$ is not a sum of two rational squares. Suppose that

$$-\beta = (\gamma/\epsilon)^2 + (\delta/\epsilon)^2,$$

where γ, δ, ϵ are integers and ϵ has no factor >1 in common with both γ and δ. Then β divides $-\beta\epsilon^2=\gamma^2+\delta^2$ and hence divides both γ and δ by the lemma. Write $\gamma=\gamma_1\beta$, $\delta=\delta_1\beta$. Then $-\epsilon^2=\beta(\gamma_1^2+\delta_1^2)$. Hence β divides ϵ^2+0^2 and hence also ϵ by the lemma. Since ϵ has the factor β in common with both γ and δ, $\beta=\pm 1$. For $\beta=+1$, $-\beta$ is not a sum of two rational squares. Hence D is a division algebra unless $\beta=-1$.

The case $\beta=-3$.—We saw that S has the basis $1, i, E, G$, with G defined by (38). Hence every integral element is of the form

$$q=x_0+x_1i+x_2E+x_3G,$$

where the x_i are integers. Let $h=h_0+\ldots+h_3G$ be any element of D. Then if m is a positive integer, the coefficients of $1, i, E, iE$ in $h-mq$ are

$$d_0=h_0+\tfrac{1}{2}h_3-m(x_0+\tfrac{1}{2}x_3), \qquad d_1=h_1+\tfrac{1}{2}h_3-m(x_1+\tfrac{1}{2}x_3),$$
$$d_2=h_2+\tfrac{1}{2}h_3-m(x_2+\tfrac{1}{2}x_3), \qquad d_3=\tfrac{1}{2}(h_3-mx_3).$$

By choice of integers x_3, x_2, x_1, x_0, we see that $d_0, \ldots, d_3$ can be made numerically $\leqq\frac{1}{2}m, \frac{1}{2}m, \frac{1}{2}m, \frac{1}{4}m$, respectively. But

$$N\equiv N(h-mq)=d_0^2+d_1^2+\beta(d_2^2+d_3^2).$$

For $\beta=-3$, $\beta(d_2^2+d_3^2)$ lies between $-\frac{15}{16}m^2$ and 0. Also, $d_0^2+d_1^2$ lies between 0 and $\frac{1}{2}m^2$. Hence N lies between $-m^2$ and $+m^2$. Then as in Lemma 2 of § 91 we can always perform the two kinds of division each with a remainder whose norm is numerically less than the norm of the divisor. From $N(q)=\pm 1$, we see that the number of units is infinite.

The case $\beta=+3$.—Employing the set S_1 with the basis $1, i, H_2, H_5$, we obtain as in Lemma 1 of § 91

$$N(h-mq)\leqq(\tfrac{1}{2}m)^2+(\tfrac{1}{2}m)^2+3(\tfrac{1}{4}m)^2+3(\tfrac{1}{4}m)^2=\tfrac{1}{16}m^2<m^2.$$

Then Lemma 2 of § 91 holds. From the integral solutions of $4N(q)=4$, we obtain at once the 12 units of D:

$$\pm 1,\quad \pm i,\quad \pm H_2,\quad \pm(H_2-i),\quad \pm H_5,\quad \pm(H_5-1).$$

Thus D is not equivalent to the algebra in the preceding case, while neither is equivalent to the algebra of rational quaternions which has 24 units.

The reader acquainted with the elements of the theory of numbers will find no difficulty in developing for algebra D with $\beta=\pm 3$ an arithmetical theory analogous to that for quaternions in § 91.

106. Application to Diophantine equations. By way of example consider $x_1^2+\ \ldots\ .\ +x_5^2=x_6^2$. By factoring $x_6^2-x_5^2$, we reduce this equation to

$$x^2+y^2+z^2+w^2=uv. \tag{42}$$

Since the norm $x^2+y^2+z^2+w^2$ of the product

$$x+yi+zj+wk=AB \tag{43}$$

of two quaternions

$$A=a+bi+cj+dk,\qquad B=\alpha+\beta i+\gamma j+\delta k \tag{44}$$

is equal to the product of their norms, (42) has the solutions

$$\begin{cases} x=a\alpha-b\beta-c\gamma-d\delta, & y=a\beta+b\alpha+c\delta-d\gamma, \\ z=a\gamma-b\delta+c\alpha+d\beta, & w=a\delta+b\gamma-c\beta+d\alpha, \\ u=a^2+b^2+c^2+d^2, & v=\alpha^2+\beta^2+\gamma^2+\delta^2. \end{cases} \tag{45}$$

We shall first find all rational solutions of (42). If $v \neq 0$, we may evidently write

$$\frac{x}{v}=\frac{a}{\alpha}, \quad \frac{y}{v}=\frac{b}{\alpha}, \quad \frac{z}{v}=\frac{c}{\alpha}, \quad \frac{w}{v}=\frac{d}{\alpha},$$

where α, a, b, c, d are integers without a common factor >1. Then

$$\frac{u}{v}=\left(\frac{x}{v}\right)^2+\ldots\ldots+\left(\frac{w}{v}\right)^2=\frac{a^2+b^2+c^2+d^2}{\alpha^2}.$$

Denote the rational number v/α^2 by f. Then

$$(46) \qquad \begin{cases} x=fa\alpha, & y=fb\alpha, \quad z=fc\alpha, \quad w=fd\alpha, \\ u=f(a^2+b^2+c^2+d^2), & v=f\alpha^2. \end{cases}$$

The rational solutions of (42) with $v=0$ have $x=y=z=w=0$ and hence are given by (46) with $\alpha=0$. The products of an arbitrary rational number f by the six numbers (45), in which $a, \ldots\ldots, \delta$ are integers without a common factor >1, give all the rational solutions of (42). In fact, we just proved that they are all given by (46) to which the products of f by the numbers (45) reduce when $\beta=\gamma=\delta=0$.

To prove that we obtain all integral solutions when we restrict the multiplier f to integral values, we have merely to show that, when the products of the numbers (45) by an irreducible fraction n/p are equal to integers, so that the numbers (45) are all divisible by p, then the quotients are expressible in the same form (45) with new integral parameters in place of $a, \ldots\ldots, \delta$. It is sufficient to prove this for the (equal or distinct) prime factors of p, since after each of them has been divided out in turn p itself has been divided out.

Hence let p be a prime which divides the six numbers (45). In particular, p divides the norm u of the quaternion A having integral co-ordinates. By Lemma 3 of § 91, A has in common with p a right divisor not a unit. By Theorem 4, p is a product $PP'=P'P$ of two conjugate prime quaternions with integral co-ordinates. After choice of the notation between P and P', we have $A=QP$, where Q is an integral quaternion.

i) Let $p>2$. Then Q has integral co-ordinates. Otherwise $Q=\frac{1}{2}q$, in which the four co-ordinates of q are all odd integers, and

$$AP'=QPP'=\tfrac{1}{2}qp=\tfrac{1}{2}p\cdot q$$

does not have integral co-ordinates in contradiction with the fact that A and P' and hence also AP' have integral co-ordinates.

Since x, y, z, w are divisible by p by hypothesis, (43) shows that $AB=pC$, where the quaternion C has integral co-ordinates. Either B has P' as a left divisor and $B=P'q$, where as above q has integral co-ordinates, or else the greatest common left divisor of B and P' is unity, so that $1=BD+P'E$, where D and E are integral quaternions. In the latter case,

$$A=A\cdot BD+A\cdot P'E=pC\cdot D+Q\cdot PP'\cdot E=p(CD+QE),$$

where $CD+QE$ is an integral quaternion, so that its double is a quaternion R having integral co-ordinates. Hence $2A=pR$, whereas the co-ordinates of A may be assumed to be not all divisible by p. For, if a, b, c, d are all divisible by p, then α, β, γ, δ are not all divisible by p and we may employ from the outset the conjugate $B'A'$ of AB in place of AB in (43). Hence the second

of the foregoing cases is excluded and we have $B=P'q$. Thus

$$A=QP, \qquad Q=a_1+b_1i+c_1j+d_1k, \qquad u=N(A)=p(a_1^2+\ \ldots\ .+d_1^2)$$

$$B=P'q, \qquad q=\alpha_1+\beta_1 i+\gamma_1 j+\delta_1 k, \qquad v=N(B)=p(\alpha_1^2+\ \ldots\ .+\delta_1^2),$$

where $a_1, \ldots, \delta_1$ are integers. Then by (43),

$$AB=QPP'q=pQq, \qquad \frac{x}{p}+\frac{y}{p}i+\frac{z}{p}j+\frac{w}{p}k=Qq.$$

Just as equations (45) were obtained from (43), we now see that the expressions for x/p, y/p, z/p, w/p, u/p, v/p are derived from the expressions in (45) by replacing $a, \ldots, \delta$ by the eight new integral parameters $a_1, \ldots, \delta_1$. This completes the proof for any odd prime p.

ii) Let $p=2$. Since u is divisible by 2, $a+b+c+d$ is even. Hence at least one of $a+b$, $a+c$, $a+d$ is even. These three cases differ only in notation since the substitution $T=(bcd)(\beta\gamma\delta)(yzw)$, which permutes b, c, d cyclically, etc., leaves unaltered* the system of equations (45). Hence we may assume that $a+b$ is even, whence $c+d$ is even. Then

$$A=a-b+b(1+i)+(c-d)j+dk(1+i)$$

is evidently the product of a quaternion Q having integral co-ordinates by $P=1+i$, since $2=(1-i)P$. Similarly, if $\alpha+\beta$ is even, $B=P'q$ and the last part of case (i)

* This is due to the fact that T corresponds to the cyclic substitution (ijk) on the units, which leaves unaltered their multiplication table (§ 11).

leads to the same conclusion when $p=2$. But if $\alpha+\beta$ is odd, $\gamma+\delta$ is odd and either $\alpha+\gamma$ or $\alpha+\delta$ is even. These two sub-cases are interchanged when we replace a by b, b by $-a$, γ by $-\delta$, and δ by γ, whence z and w in (45) remain unaltered, while x is replaced by y, and y by $-x$. Hence let $\alpha+\gamma$ be even. Since $a+b$ and $c+d$ are even, while $\alpha+\beta$ and $\gamma+\delta$ are odd,

$$0\equiv x\equiv a\alpha+a(\alpha+1)-c\gamma+c(\gamma+1)\equiv a+c \pmod 2.$$

Applying the inverse substitution T^{-1} to $a+c$ and $\alpha+\gamma$, we are led to the former case in which $a+b$ and $\alpha+\beta$ are even.

THEOREM. *All integral solutions of* $x^2+y^2+z^2+w^2=uv$ *are given by the products of the numbers* (45) *by an arbitrary integer and hence are given by the formula which expresses the fact that the norm of the product of two quaternions is equal to the product of their norms.*

This simple method due to the author* has led to the complete solution in integers of various Diophantine equations not previously solved completely. It is evidently applicable to $x^2+y^2\pm 3(z^2+w^2)=uv$ since there exists a greatest common left (or right) divisor of any two integral elements of the algebra D of § 105 with $\beta=\pm 3$.

In his book (cited in § 91), Hurwitz employed quaternions to prove classic theorems on the number of ways of expressing a positive integer as a sum of four integral squares and to prove that every real linear transformation

$$y_i=a_{i1}x_1+\ \ldots\ .\ .\ .\ .\ +a_{i4}x_4 \qquad (i=1,\ 2,\ 3,\ 4)$$

* *Comptes Rendus du Congrès International des Mathématiciens* (Strasbourg, 1920) pp. 46–52. Further developed in *Bulletin of the American Mathematical Society*, XXVII (1921), 353–65.

of positive determinant for which $\Sigma y_i^2 = c\Sigma x_i^2$ may be obtained from the equation $y = axb$ between real quaternions. In particular, for $c = 1$, every real orthogonal transformation of determinant $+1$ on four variables is obtained from $y = axb$ where the norms of the quaternions a and b are unity. To obtain corresponding results for three variables, take $y_1 = x_1 = 0$, $b = a'$.

CHAPTER XI

FIELDS

107. Examples. In § 1 we gave several examples of fields of ordinary complex numbers. There exist also fields of functions; one example is the set of all rational functions of a variable x with rational coefficients; a more general example is the set of all rational functions of the independent complex variables $x_1, \ldots, x_n$ having as coefficients numbers belonging to any chosen field of complex numbers.

Still further types of fields are obtained if we adopt the purely abstract definition next explained.

We shall treat only those properties of fields which are required to make the theory of algebras presented in the preceding chapters valid for algebras over an arbitrary field.

108. Postulates* for a field. A field F is a system consisting of a set S of elements $a, b, c, \ldots$ and two operations, called addition and multiplication, which may be performed upon any two (equal or distinct) elements a and b of S, taken in that order, to produce uniquely determined elements $a \oplus b$ and $a \odot b$ of S, such that postulates I–V are satisfied. For simplicity, we shall write $a+b$ for $a \oplus b$, and ab for $a \odot b$, and call them the *sum* and *product*, respectively, of a and b. Moreover, elements of S will be called elements of F.

* Essentially the second set by Dickson, *Transactions of the American Mathematical Society*, IV (1903), 13–20. For other definitions by him and by Huntington, see *ibid.*, VI (1905), 181–204.

I. If a and b are any two elements of F, $a+b$ and ab are uniquely determined elements of F, and

$$b+a=a+b, \qquad ba=ab.$$

II. If a, b, c are any three elements of F,

$$(a+b)+c=a+(b+c), \qquad (ab)c=a(bc), \qquad a(b+c)=ab+ac.$$

III. There exist in F two distinct elements, denoted by 0 and 1, such that if a is any element of F, $a+0=a$, $a\cdot 1=a$ (whence $0+a=a$, $1\cdot a=a$ by I).

IV. Whatever be the element a of F, there exists in F an element x such that $a+x=0$ (whence $x+a=0$ by I).

V. Whatever be the element a (distinct from 0) of F, there exists in F an element y such that $ay=1$ (whence $ya=1$ by I).

109. Simple properties; subtraction and division.

VI. The elements denoted by 0 and 1 in III are unique and will be called the *zero* and the *unity* of F.

For, if $a+z=a$ and $au=a$ for every a in F, we have in particular $0+z=0$, $1\cdot u=1$. But, by III, $0+z=z$, $1\cdot u=u$. Hence $z=0$, $u=1$.

VII. If a, b, c are elements of F such that $a+b=a+c$, then $b=c$.

For, by IV, there exists an element x of F such that $x+a=0$. Using also II_1, we get

$$b=0+b=(x+a)+b=x+(a+b)=x+(a+c)$$
$$=(x+a)+c=0+c=c.$$

In particular, if $a+b=0$ and $a+c=0$, then $b=c$. Hence the element x in IV is uniquely determined by a; it will be designated by $-a$.

VIII. If a and b are any elements of F, there exists one and (by VII) only one element x of F for which $a+x=b$, viz., $x=-a+b$. For,

$$a+[-a+b]=[a+(-a)]+b=0+b=b\,.$$

The resulting element x will be written $b-a$ and called the result of *subtracting* a from b.

IX. If a, b, c are elements of F such that $ab=ac$ and $a\neq 0$, then $b=c$.

For, by V, there exists an element y of F such that $ya=1$. Using also II_2, we get

$$b=1\cdot b=(ya)b=y(ab)=y(ac)=(ya)c=1\cdot c=c\,.$$

In particular, if $ab=1$ and $ac=1$, then $b=c$. Hence the element y in V is uniquely determined by a; it is called the *reciprocal* (or *inverse*) of a and designated by $1/a$ or a^{-1}.

By II_3 with $c=0$ and VII, $a0=0$. Taking $c=0$ in IX, we see that $ab=0$, $a\neq 0$, imply $b=0$.

X. If a and b are elements of F and $a\neq 0$, there exists one and (by IX) only one element x of F such that $ax=b$, viz., $x=a^{-1}b$.

For,

$$a(a^{-1}b)=aa^{-1}\cdot b=1\cdot b=b\,.$$

The resulting element x will be designated by b/a and called the *quotient* of b by a, or the result of *dividing* b by a.

110. Example of a finite field. Let p be a prime number >1. All integers a, $a\pm p$, $a\pm 2p$, ... which differ from a by a multiple of p are said to form a *class of residues* $[a]$ *modulo* p, and this class may also be designated by $[a+kp]$, where k is any integer. Hence

there are exactly p distinct classes: [0], [1], ... , $[p-1]$. We shall take them as the p elements of a finite field F in which addition and multiplication are defined by

$$[a]+[a']=[a+a'], \qquad [a][a']=[aa'].$$

To justify these definitions, note that if k and l are any integers, the sum and product of $a+kp$ and $a'+lp$ are, respectively, $a+a'+mp$ and $aa'+tp$, where $m=k+l$, $t=al+a'k+klp$. In other words, whichever number of class $[a]$ we add to whichever number of class $[a']$, we always obtain a number of the same class $[a+a']$; and similarly for multiplication.

For these p elements and for addition and multiplication just defined, it is easily seen that the postulates I–IV for a field are all satisfied. Classes [0] and [1] are the zero and unity elements, respectively. Postulate V states that if $[a]$ is any class $\neq[0]$, there exists a class $[y]$ such that $[a][y]=[1]$, and is another statement of the well-known theorem that, if a is any integer not divisible by the prime p, there exist integers y and z such that $ay=1+pz$. For example, if $p=5$, $a=2$, 3, or 4, then

$$2\cdot 3=1+5\cdot 1=3\cdot 2, \qquad 4\cdot 4=1+5\cdot 3.$$

To prove the last theorem, assign to y the values 1, 2, ... , $p-1$, and divide each product ay by p to obtain a remainder >0 and $<p$. Since the $p-1$ remainders are distinct, they must be 1, 2, ... , $p-1$ in some order. Hence one remainder is 1, as desired.

111. Indeterminates and polynomials in them. We shall first define a single indeterminate x and polynomials

(1) $$a_0+a_1x+ \ldots . +a_nx^n$$

in x having as coefficients elements $a_0, \ldots . , a_n$ of any field F.

We consider simultaneously for $n=0, 1, 2, \ldots .$ all sets

$$a=(a_0, a_1, \ldots . , a_n)$$

of $n+1$ ordered elements $a_0, a_1, \ldots . , a_n$ of F. The set

$$b=(\beta_0, \beta_1, \ldots . , \beta_m), \qquad m \geqq n,$$

shall be called equal to the set a if and only if

$$\beta_i=a_i \ (i=0, 1, \ldots . , n), \qquad \beta_j=0 \ (j=n+1, \ldots . , m).$$

The sum $a+b$ of a and b is defined to be the set

$$(a_0+\beta_0, \ldots . , a_n+\beta_n, \beta_{n+1}, \ldots . , \beta_m).$$

The product ab is defined to be $(\gamma_0, \gamma_1, \ldots . , \gamma_{n+m})$, where

$$\gamma_0=a_0\beta_0, \ \gamma_1=a_0\beta_1+a_1\beta_0, \ \ldots . , \ \gamma_k=\sum_{i=0}^{k} a_i\beta_{k-i}, \ \ldots . .$$

In particular, for sets composed of single elements,

$$(a)+(\beta)=(a+\beta), \qquad (a)(\beta)=(a\beta).$$

Hence these sets form a field which is abstractly identical with F, so that no contradiction can arise if we identify (a) with a. Accordingly, if ρ is any element of F we define (ρ) to be ρ. Then

$$\rho a=a\rho=(\rho)a=a(\rho)=(\rho a_0, \ldots . , \rho a_n).$$

Denote the set $(0, 1)$ by x. Then

$$x^2=(0, 0, 1), \qquad x^k=(0, \ldots . , 0, 1),$$

in which 1 is preceded by k zeros. Hence

$$(a_0, a_1, \ldots, a_n) = (a_0) + (0, a_1) + (0, 0, a_2) + \ldots$$
$$= a_0 + a_1(0, 1) + a_2(0, 0, 1) + \ldots$$

takes the form (1) above, which is called a *polynomial* in the *indeterminate* $x = (0, 1)$ with coefficients $a_0, \ldots, a_n$ in F.

Two such polynomials are therefore equal only when corresponding coefficients are equal, while their sum and product are found exactly as in elementary algebra.

If $a_n \neq 0$, polynomial (1) is said to be of *degree* n in x. No degree is assigned if $a_0 = 0, \ldots, a_n = 0$. The degree of the product of two polynomials in x is evidently the sum of their degrees. Hence the product is zero only when at least one polynomial factor is zero.

To define polynomials in two indeterminates x and y, consider sets $s = [a_0, a_1, \ldots, a_n]$ of $n+1$ ordered polynomials

$$a_0 = c_{00} + c_{01}x + c_{02}x^2 + \ldots,$$
$$\ldots, \quad a_n = c_{n0} + c_{n1}x + c_{n2}x^2 + \ldots$$

in x with coefficients c_{ij} in F. Define equality, addition, and multiplication of sets exactly as above. Write y for the set $[0, 1]$. As above,

$$s = a_0 + a_1 y + \ldots + a_n y^n = \sum_{i=0}^{n} (c_{i0} + c_{i1}x + c_{i2}x^2 + \ldots) y^i.$$

The final sum is called a polynomial in the two indeterminates x and y with coefficients c_{ij} in F.

The method just employed to define polynomials in two indeterminates by means of those in one may be used to define polynomials in k (commutative) indeter-

minates $x_1, \ldots, x_k$ by means of those in $x_1, \ldots, x_{k-1}$. By induction on k we obtain the

THEOREM. *Two polynomials in the indeterminates $x_1, \ldots, x_k$ with coefficients in F are equal only when corresponding coefficients are equal. Their sum and product are found as in elementary algebra. Their product is zero only when at least one of them is zero. All operations on polynomials in indeterminates are in their last analysis operations on sets of ordered elements of the given field F.*

If f, g, h are polynomials in $x_1, \ldots, x_k$ with coefficients in F such that $f=gh$, then f is said to be *divisible* by g and h. Then if neither g nor h is an element of F, f is called *reducible* with respect to F. But if f has no divisor other than a and af, where a is an element $\neq 0$ of F, f is called *irreducible* with respect to F.

For example, $x_1^2-4x_2^2$ is reducible and $x_1^2-3x_2^2$ is irreducible with respect to the field of rational numbers.

112. Polynomials which vanish throughout F. We shall consider first a polynomial $f(x)$ of degree $n>0$ in one indeterminate x with coefficients in the field F. If e is an element of F, we have

$$x^k=(x^{k-1}+x^{k-2}e+x^{k-3}e^2+ \ldots +xe^{k-2}+e^{k-1})(x-e)+e^k.$$

Multiply by the coefficient a_k of x^k in $f(x)$ and sum as to k. We get $f(x)=Q(x)(x-e)+f(e)$, where $Q(x)$ is a polynomial of degree $n-1$ in x with coefficients in F. When the element $f(e)$ of F is zero, we shall say that $f(x)$ *vanishes for* e and has the *divisor* $x-e$.

Let $f(x)$ vanish for two distinct elements e_1 and e_2 of F. From

$$f(x)=(x-e_1)Q(x), \qquad 0=(e_2-e_1)Q(e_2)=0,$$

we have $Q(e_2)=0$, so that $Q(x)$ has the divisor $x-e_2$. Thus $f(x)=(x-e_1)(x-e_2)Q_1(x)$. A repetition of this argument shows that, if $f(x)=a_0x^n+\ \ldots\ .$ vanishes for n distinct elements $e_1, \ldots, e_n$ of F, then

$$f(x)=a_0(x-e_1)(x-e_2)\ \ldots\ .\ (x-e_n).$$

If $f(x)$ vanishes also for e which is distinct from $e_1, \ldots, e_n$, then $a_0=0$. Repeating the argument on $a_1x^{n-1}+\ \ldots\ .$, etc., we obtain the following conclusion:

I. *If a polynomial $a_0x^n+\ \ldots\ .+a_n$ with coefficients in F vanishes for more than n elements of F, each coefficient a_i is zero.*

II. *In any infinite field F, a polynomial in x with coefficients in F is zero (identically) if it vanishes for all elements of F.*

But II need not hold for a finite field. For example, if F is the field of the classes of residues of integers modulo p, a prime (§ 110), the polynomial x^p-x is not zero, but vanishes for every element of F since, by Fermat's theorem, e^p-e is divisible by p when e is any integer.

III. *A polynomial $f(x_1, \ldots, x_n)$ in n indeterminates with coefficients in an infinite field F is zero (identically) if it vanishes for all sets of n elements of F.*

To give a proof by induction, let III be true for polynomials in $x_1, \ldots, x_{n-1}$. Then III is true for f if it lacks x_n. Hence let

$$f=g_0(x_1, \ldots, x_{n-1})x_n^m+\ \ldots\ .+g_m(x_1, \ldots, x_{n-1}),\qquad g_0\neq 0,\quad m\geqq 1.$$

In view of the hypothesis for the induction, we may assign elements $\xi_1, \ldots, \xi_{n-1}$ of F such that $g_0(\xi_1,$

. . . . , $\xi_{n-1}) \neq 0$. Then f becomes a polynomial in the single indeterminate x_n, which, by II, does not vanish for a certain element e of F. But this contradicts the assumption that f vanishes for the set of elements $\xi_1, \ldots, \xi_{n-1}, e$.

113. Laws of divisibility of polynomials in x. It is to be understood that all the polynomials employed have their coefficients in any fixed field F.

We shall first prove that there exists a greatest common divisor of any two polynomials $f(x)$ and $h(x)$, the latter being of degree $n > 0$. The process employed in elementary algebra to divide $f(x)$ by $h(x)$ is purely rational and hence leads to a quotient $q_1(x)$ and a remainder $r_1(x)$, each being a polynomial with coefficients in F, such that either $r_1(x)$ is zero (and then f is exactly divisible by h) or $r_1(x)$ has a degree $n_1 (n_1 < n)$. In either case,

$$f(x) = h(x)q_1(x) + r_1(x).$$

If $r_1(x) \neq 0$, we divide $h(x)$ by $r_1(x)$ and obtain a quotient $q_2(x)$ and a remainder $r_2(x)$ which is either zero or has a degree $n_2 (n_2 < n_1)$, whence

$$h(x) = r_1(x)q_2(x) + r_2(x).$$

If $r_2(x) \neq 0$, we repeat the process on r_1 and r_2, and get

$$r_1(x) = r_2(x)q_3(x) + r_3(x).$$

Since $n, n_1, n_2, \ldots$ form a series of decreasing integers $\geqq 0$, the process must terminate and ultimately lead to a remainder r_{m+1} which is zero, while $r_m \neq 0$. The final equations of the series are therefore

$$r_{m-2}(x) = r_{m-1}(x)q_m(x) + r_m(x),$$
$$r_{m-1}(x) = r_m(x)q_{m+1}(x).$$

Employing these equations in reverse order, we see that $r_m(x)$ divides $r_{m-1}(x)$, $r_{m-2}(x)$, ... , $r_3(x)$, $r_2(x)$, $r_1(x)$, $h(x)$, $f(x)$, and hence is a common divisor of the given polynomials f and h.

Conversely, employing the equations in their original order, we see that any common divisor of f and h is a divisor of $r_1, r_2, \ldots, r_{m-2}, r_{m-1}, r_m$.

Hence the common divisors of f and h coincide with the divisors of $r_m(x)$, which is therefore called a greatest common divisor of f and h. Let $g(x)$ be any greatest common divisor of f and h, i.e., a common divisor which is divisible by every common divisor. Then $g(x)$ and $r_m(x)$ divide each other, whence $g(x) = ar_m(x)$, where a is an element $\neq 0$ of the field F.

From the first two equations above, we get

$$r_1 = f - q_1 h, \qquad r_2 = -q_2 f + (1 + q_1 q_2) h.$$

Inserting these values into the third equation, we get

$$r_3 = (1 + q_2 q_3) f - [q_1 + q_3(1 + q_1 q_2)] h.$$

It follows by induction on j that r_j is a linear homogeneous function of f and h whose coefficients are polynomials in x. The same is therefore true of $g(x) = ar_m(x)$.

We have now proved the following theorem:

I. *If $f(x)$ and $h(x)$ are any polynomials in an indeterminate x with coefficients in any field F, such that f and h are not both zero, they have a greatest common divisor $g(x)$, with coefficients in F, which is uniquely determined up to a factor $\neq 0$ belonging to F. There exist two polynomials $s(x)$ and $t(x)$ having coefficients in F such that*

$$g(x) = s(x) f(x) + t(x) h(x). \tag{2}$$

In case $g(x)$ reduces to an element $\gamma \neq 0$ of F, we shall call $f(x)$ and $h(x)$ *relatively prime.* In that case, we multiply the terms of (2) by δ, where $\gamma\delta = 1$, and write $\sigma(x) = \delta s(x)$, $\tau(x) = \delta t(x)$. Hence if f and h are relatively prime, there exist polynomials σ and τ with coefficients in F such that

$$1 = \sigma(x)f(x) + \tau(x)h(x). \tag{3}$$

Multiplying (3) by $k(x)$, we deduce

II. *If $f(x)$ and $h(x)$ are relatively prime, and if the product $f(x)k(x)$ is divisible by $h(x)$, then $k(x)$ is divisible by $h(x)$.*

If both $f(x)$ and $l(x)$ are relatively prime to $h(x)$, we have (3) and $1 = s(x)l(x) + t(x)h(x)$. By multiplication,

$$1 = \sigma sfl + (\sigma ft + \tau sl + \tau ht)h,$$

which shows that fl is relatively prime to h. This implies

III. *If two or more polynomials in x are each relatively prime to $h(x)$, their product is relatively prime to $h(x)$.*

A polynomial is evidently either divisible by an irreducible polynomial or else is relatively prime to it. Hence III implies

IV. *If the product of two or more polynomials is divisible by an irreducible polynomial $h(x)$, at least one of them is divisible by $h(x)$.*

A reducible polynomial $f(x)$ is by definition the product of two polynomials $f_1(x)$ and $f_2(x)$ each of degree $\geqq 1$. If $f_i(x)$ is reducible, we replace it by a product of two polynomials each of degree $\geqq 1$. Proceeding in this manner, we obtain a factorization

$$f(x) = p_1(x)p_2(x) \ldots . p_k(x)$$

of $f(x)$ into irreducible polynomials each of degree $\geqq 1$ and having all coefficients in F. If there were a second such factorization

$$f(x)=q_1(x)q_2(x)\ \ldots\ q_r(x),$$

the latter product of irreducible polynomials $q_i(x)$ would be divisible by $p_1(x)$, whence, by IV, a certain $q_i(x)$ would be divisible by $p_1(x)$. After relabeling the q's, we may take $i=1$. Then $q_1(x)=a_1p_1(x)$, where a_1 is an element $\neq 0$ of F. Thus

$$p_1(x)[p_2(x)\ \ldots\ p_k(x)-a_1q_2(x)\ \ldots\ q_r(x)]=0.$$

Hence the second factor is zero. As before, $p_2(x)$ would divide one of the q_i, $i\geqq 2$, say q_2, whence $q_2=a_2p_2$. Proceeding similarly, we obtain

V. *Any polynomial reducible in F can be expressed as a product of polynomials irreducible in F; apart from the arrangement of the polynomials and the association of multipliers belonging to F, this factorization can be effected in a single way.*

The theorems of this section are illustrated in § 116 for the case of congruences with respect to a prime modulus.

114. Laws of divisibility of polynomials in several indeterminates. The theorems of this section are stated explicitly for polynomials in two indeterminates x and y. However, if we interpret x to mean a set of indeterminates $x_1, \ldots, x_n$, the theorems concern polynomials in $x_1, \ldots, x_n, y$ and are established by induction from n to $n+1$ variables by the proofs as written,* if we assume that Theorems V, VII, VIII hold

* Provided the citations to I, IV, V of § 113 be replaced by citations to the analogues of V, VII, VIII below for polynomials in $x_1, \ldots, x_n$.

for polynomials in $x_1, \ldots, x_n$. Since the latter theorems were proved in § 113 when $n=1$, the induction will be complete.

If $\rho_i(x)$ and $\sigma_i(x)$ are polynomials in x with coefficients in F,

$$(4) \quad r(x, y)=\sum_{i=0}^{n}\rho_i(x)y^i, \qquad \rho_n(x)\neq 0;$$

$$s(x, y)=\sum_{i=0}^{m}\sigma_i(x)y^i, \qquad \sigma_m(x)\neq 0$$

are of degrees n and m, respectively, in y. By I of § 113, $\rho_0(x), \ldots, \rho_n(x)$ have a greatest common divisor $\rho(x)$. In case $\rho(x)$ reduces to an element of F, we call $r(x, y)$ *primitive in* y. Let $\sigma(x)$ be a greatest common divisor of $\sigma_0(x), \ldots, \sigma_m(x)$. Then

$$(5) \qquad r(x, y)=\rho(x)R(x, y), \qquad s(x, y)=\sigma(x)S(x, y),$$

where R and S are primitive in y.

I. *If the product of* $r(x, y)$ *and* $s(x, y)$ *is divisible by a polynomial* $P(x)$ *which is irreducible in* F, *either* r *or* s *is divisible by* $P(x)$.

Since this is evident if every $\rho_i(x)$ or every $\sigma_i(x)$ in (4) is divisible by $P(x)$, let $\rho_p(x)$ and $\sigma_q(x)$ be relatively prime to $P(x)$, and $\rho_i(x)$ and $\sigma_j(x)$ be divisible by $P(x)$ for $i>p, j>q$. Then

$$rs=\sum_{i=0}^{p}\rho_i(x)y^i \cdot \sum_{i=0}^{q}\sigma_i(x)y^i+P(x)Q(x, y).$$

Since rs is divisible by $P(x)$, the coefficient $\rho_p(x)\sigma_q(x)$ of y^{p+q} must be divisible by $P(x)$, contrary to IV of § 113.

II. *If two polynomials* $r(x, y)$ *and* $s(x, y)$ *are primitive in* y, *their product is primitive in* y.

For, if rs is not primitive in y, then $rs=\tau(x)T(x, y)$, where $\tau(x)$ is not an element of F and hence, by V of § 113, has a factor $P(x)$ which is irreducible in F. Then, by I, either r or s is divisible by $P(x)$, whereas each is primitive in y.

III. *If, in* (5), *R and S are primitive in y and if r is divisible by s, then R is divisible by S, and* $\rho(x)$ *is divisible by* $\sigma(x)$.

For, if $r=sk$, where $k=\kappa(x)K(x, y)$ and K is primitive in y, then

$$r=\sigma\kappa SK, \qquad r=\rho R.$$

Since SK is primitive in y by II, a greatest common divisor of the coefficients of the powers of y in r is $\sigma\kappa$ by the first equation and is ρ by the second. Hence, by I of § 113, $\sigma\kappa=a\rho$, where a is in F. Then $R=aSK$.

COROLLARY *Any divisor of a polynomial primitive in y is itself primitive in y*

This proof establishes also

IV. *If* $\rho(x)R$ *is equal to the product of* $\sigma(x)S$ *by* $\kappa(x)K$, *where R, S, K are primitive in y, then* $R=aSK$ *and* $\sigma\kappa=a\rho$, *where a is an element of F.*

V. *Two polynomials* $r(x, y)$ *and* $s(x, y)$ *with coefficients in F have a greatest common divisor* $[r, s]$ *which is uniquely determined apart from a factor belonging to F. The product* of* $[r, s]$ *by a certain polynomial in x is expressible as a linear combination of r and s, while* $[r, s]$ *itself may not be so expressible.*

* For example, let $r=(x+1)y-1$, $s=x(y+1)$, and let F be the field of rational numbers. Evidently $[r, s]=1$, which is not a linear combination of r and s since they are both zero when $x=-2$, $y=-1$. This holds also if F is the field of the three classes of residues of integers modulo 3 (§ 110). Hence we cannot prove VI by the method employed for II of § 113.

For, let $s=v(x)y^n+\ \ldots\ .$ be of degree $n>0$ in y. If r is of degree $n+k-1$ in y, the algebraic division of $v^k r$ by s yields a quotient q_1 and remainder r_1 which is either zero or has a degree $n_1(n_1<n)$ in y, whence

$$v^k r=sq_1+r_1\,.$$

But if r is of degree $<n$ in y, we take $k=0$, $q_1=0$, $r_1=r$, and see that the preceding equation continues to hold.

If $n_1>0$, we write $r_1=v_1(x)y^{n_1}+\ \ldots\ .$ and find similarly that

$$v_1^{k_1}s=r_1q_2+r_2\,,$$

where r_2 is either zero or has a degree $n_2(n_2<n_1)$ in y. Since $n, n_1, n_2, \ldots .$ form a series of decreasing integers $\geqq 0$, the process terminates and ultimately leads to a remainder r_{m+1} which is zero, while $r_m\neq 0$. The final two equations of the series are

$$v_{m-1}^{k_{m-1}}r_{m-2}=r_{m-1}q_m+r_m\,,\qquad v_m^{k_m}r_{m-1}=r_mq_{m+1}\,.$$

Employ (5) and $r_m=\tau(x)T(x,\ y)$, where R, S, T are primitive in y. Any common divisor of R and S divides r and s by (5) and hence divides $r_1, r_2, \ldots , r_m$ in view of our equations. Such a divisor of R and S is primitive in y by the corollary to III. Since it divides $r_m=\tau T$, it divides T by III.

Conversely, any divisor of T is primitive in y by the corollary. Since it divides $v_m^{k_m}r_{m-1}$, it divides r_{m-1}. Similarly, it is a divisor of $r_{m-2}, \ldots , r_2, r_1, s, r$, and hence of R and S.

The two results show that $T=[R,\ S]$. Then, by III,

$$[r,\ s]=[\rho,\ \sigma]T\,.$$

In case $[r, s]$ is an element of F, r and s are called *relatively prime.*

VI. *If $r(x, y)$ and $s(x, y)$ are relatively prime and if $r \cdot k(x, y)$ is divisible by s, then k is divisible by s.*

For, s is a divisor of both rk and sk, and hence of

$$[rk, sk] = [r, s]k = ak, \qquad a \text{ in } F.$$

VII. *If the product of two or more polynomials in x and y is divisible by a polynomial $s(x, y)$ which is irreducible in F, at least one of them is divisible by s.*

For, if rk is divisible by s, and r is not, then r and s are relatively prime. Then, by VI, k is divisible by s.

VIII. *Unique factorization into irreducible polynomials follows as in* V *of* § 113.

115. Algebraic extension of any field. In § 1 we employed a root α of an algebraic equation having rational coefficients and noted that the rational functions of α with rational coefficients form the algebraic number field $R(\alpha)$, which may be regarded as the algebraic extension of the field R of all rational numbers by the adjunction of α. We may replace R by any other subfield S of the field of all complex numbers, employ a root α (existing as a complex number) of an algebraic equation with coefficients in S, and conclude that the rational functions of α with coefficients in S form a field $S(\alpha)$.

But the preceding method cannot be applied directly to a field F not of type S, since we have, as yet, attached no meaning to the term root of an equation with coefficients in F (apart from special cases in which there is a root in F). We shall reach the corresponding goal by a different method.

Let $P(x)$ be a polynomial of degree $n \geqq 1$ in the indeterminate x. This and all further polynomials to be employed are understood to have all their coefficients in the (arbitrary) field F.

Two polynomials $g_1(x)$ and $g_2(x)$ are called *congruent modulo* $P(x)$ if $g_1 - g_2$ is divisible by $P(x)$; we then write $g_1 \equiv g_2 \pmod{P}$. All polynomials which are congruent to a given one g are said to form the class $[g]$. The zero class $[0]$ is composed of all polynomials, including 0, which are divisible by P.

If also $h_1(x) \equiv h_2(x) \pmod{P}$, then

$$g_1 + h_1 \equiv g_2 + h_2, \qquad g_1 h_1 \equiv g_2 h_2 \pmod{P}.$$

Hence the sum of an arbitrary polynomial $g_i(x)$ of a class G and an arbitrary polynomial $h_j(x)$ of a class H belongs to a class uniquely determined by G and H, and is designated by either $G+H$ or $H+G$. Also their product belongs to a definite class designated by GH or HG. In other words, addition and multiplication of classes are defined by

$$(6) \qquad [g]+[h]=[h]+[g]=[g+h], \qquad [g][h]=[h][g]=[gh].$$

We assume henceforth that $P(x)$ is irreducible with respect to F. If $G \neq [0]$, any polynomial $g(x)$ of G is not divisible by $P(x)$ and hence is relatively prime to the irreducible polynomial $P(x)$. Hence by (3) there exist polynomials $\sigma(x)$ and $\tau(x)$ such that $\sigma g + \tau P = 1$. But $\tau P \equiv 0 \pmod{P}$, so that $[g\sigma]=[1]$. Let S denote the class containing σ. Hence $GS=[1]$.

The postulates (§ 108) for a field are seen to be satisfied by our classes as elements under addition and multiplication as defined by (6), with $[0]$ and $[1]$ as the

zero and unity elements. Since each number a of F is a polynomial lacking x, it determines a class $[a]$, and these special classes form a field simply isomorphic with F.

THEOREM 1. *If $P(x)$ is a polynomial irreducible in F, the classes modulo $P(x)$ of polynomials with coefficients in F form a field F_1 having a sub-field simply isomorphic with F.*

Each class $\neq[0]$ is determined by the unique reduced polynomial of degree $<n$ in the class, while the class $[0]$ is determined by the polynomial 0. We may therefore employ these reduced polynomials, including 0, as the elements of F_1. Then the sum of two such elements $g(x)$ and $h(x)$ is an element of F_1, but their product is the element obtained as the remainder of degree $<n$ from the division of $g(x) \cdot h(x)$ by $P(x)$ This remainder may also be obtained by the elimination of the powers of x with exponents $\geqq n$ by means of the recursion formula $P(x)=0$. In other words, we may regard the element x of F_1 as a root of $P(\xi)=0$; this agreement is merely a convenient mode of expressing the fact that x is a root of the congruence

$$(7) \qquad P(\xi)\equiv(\xi-x)Q(\xi, x)\equiv 0 \pmod{P(x)},$$

in which the polynomial $Q(\xi, x)$ is the quotient obtained by dividing $P(\xi)$ by $\xi-x$, the remainder being $P(x)$.

We have therefore solved the problem to extend a given field F to a field F_1 containing a root of a given equation $P(x)=0$ which is irreducible in F.

For various applications we need an extension F' of a given field F such that any given polynomial $f(x)$, having coefficients in F, shall decompose into a product

of linear factors with coefficients in F'. In case there is such a decomposition in F, we may take $F'=F$. In the contrary case, $f(x)$ has an irreducible factor $P(x)$ of degree >1. In the field $F_1=F(x)$ obtained above, we have $P(\xi)=(\xi-x)Q(\xi,\ x)$, whence* $f(\xi)=(\xi-x)f_1(\xi)$, where $f_1(\xi)$ is a polynomial in ξ with coefficients in F_1.

In case $f_1(\xi)$ is a product of linear functions of ξ with coefficients in F_1, we may take F_1 as the desired field F'. In the contrary case, $f_1(y)$ has a factor $P_1(y)$ which is irreducible in F_1 and of degree >1 in the new indeterminate y. As above, y is a root of $P_1(\xi)=0$ in an extension $F_2=F_1(y)$ of F_1, so that $P_1(\xi)$ has the factor $\xi-y$ in F_2. Thus† $f_1(\xi)=(\xi-y)f_2(\xi)$, where $f_2(\xi)$ has coefficients in F_2.

If $f_2(\xi)$ is a product of linear functions of ξ with coefficients in F_2, we may take $F'=F_2$. In the contrary case, we employ a non-linear factor $P_2(\xi)$ irreducible in F_2, and extend F_2 to $F_3=F_2(z)$, where $P_2(z)=0$.

Proceeding similarly, we ultimately‡ obtain a field F' in which $f(\xi)$ is a product of linear functions of ξ.

THEOREM 2. *Given any field F and any polynomial $f(x)$ with coefficients in F, we can determine an extension F' of F such that $f(x)$ is a product of linear functions with coefficients in F'.*

116. Applications to congruences; Galois fields. Although not required for our exposition of the theory of

* This and the preceding equation are really congruences modulo $P(x)$.

† This is really a congruence modulis $P(x)$, $P_1(y)$, viz.,

$$f_1(\xi)-(\xi-y)\,f_2(\xi)=AP(x)+BP_1(y),$$

where A and B are polynomials in x and y with coefficients in F.

‡ Or by adjoining a single root of the Galois resolvent of $f(\xi)=0$, as proved by J. König (*Algebraische Grösen* [Leipzig, 1903], pp. 150–55).

algebras, an excellent illustration of the preceding theory is furnished by the case in which F is the field of classes of residues of integers modulo p, where p is a prime >1 (§ 110).

By a polynomial in an indeterminate x we shall here mean one having integral coefficients. Two such polynomials are called congruent modulo p if and only if the coefficients of like powers of x are congruent modulo p (i.e., their difference is divisible by p).

A polynomial $h(x)$, not congruent to 0, is said to be of degree n modulo p if the coefficient of x^n is prime to p and the coefficients of all higher powers of x are divisible by p. Given also any second polynomial $f(x)$, we can readily determine three polynomials q, r, s, such that

$$f(x)=h(x)q(x)+r(x)+ps(x), \tag{8}$$

where $r(x)$ is either 0 or of degree $<n$ modulo p. In case $r(x)\equiv 0 \pmod{p}$, we shall say that $f(x)$ is divisible by $h(x)$ modulo p.

Theorem I of § 113 now states that any two polynomials have a greatest common divisor modulo p which is congruent to a linear combination of the two. Again, Theorem V now states that a polynomial in x which is reducible modulo p is congruent to a product of polynomials each irreducible modulo p, and such a factorization is unique apart from the arrangement of the factors and apart from multipliers which are integers prime to p. It is unnecessary to restate similarly the remaining theorems of §§ 113–14.

Each coefficient of $r(x)$ in (8) can be expressed in the form $a+pb$, where a and b are integers and $0\leqq a<p$. The terms having the factor p may be combined with

$ps(x)$. Also replace $h(x)$ by a polynomial $P(x)$ of degree n irreducible modulo p. Then (8) becomes

$$f(x)=R(x)+pt(x)+P(x)q(x), \tag{9}$$

where

$$R(x)=a_0+a_1x+\ldots.+a_{n-1}x^{n-1} \qquad (0\leqq a_i<p). \tag{10}$$

We shall say that $f(x)$ has the ultimate residue (10) modd p, $P(x)$. All polynomials having the same ultimate residue $R(x)$ are said to form a class $[R(x)]$ modd p, $P(x)$. Hence there are p^n classes. By Theorem 1 of § 115, they form a field of order p^n, called a *Galois field* and designated by $GF[p^n]$. Its elements may be taken to be the p^n ultimate residues (10), where now the particular residue x is regarded as a (Galois imaginary) root of $P(x)=0$ in the $GF[p^n]$, as explained in § 115.

It can be proved* that, if p is any given prime and n is any given integer, there exists a polynomial $P(x)$ of degree n which is irreducible modulo P, so that the $GF[p^n]$ exists. It is uniquely determined by p and n. Every finite field is a Galois field, a theorem due to E. H. Moore.

* Dickson, *Linear Groups* (Leipzig, 1901), pp. 13–19.

APPENDIXES

APPENDIX I

DIVISION ALGEBRAS OF ORDER n^2

THEOREM.* *If no power of γ less than the nth is the norm of a polynomial in x with coefficients in F, algebra D defined by* (7) *and* (8) *of* § 47 *is a division algebra.*

We arrange the roots of $\phi(\omega)=0$ given by (5) of § 47 in the following order:

$$(1)\quad \xi_1=\xi,\quad \xi_2=\theta^{n-1}(\xi),\ \ldots,\quad \xi_i=\theta^{n-i+1}(\xi),\ \ldots,\ \xi_n=\theta(\xi),$$

whence

$$(2)\quad \theta(\xi_{i+1})=\xi_i,\qquad \xi_{n+1}\equiv\xi_1\qquad (i=1,\ \ldots,\ n).$$

Let $F(\xi)$ be the field obtained by adjoining to F one root, and hence every root (1), of $\phi(\omega)=0$. Let A be the algebra over $F(\xi)$ which has the same basal units as D. Then

$$\phi(x)=(x-\xi_1)\ \ldots\ (x-\xi_n)=0$$

in A. Write

$$(3)\quad e_{ii}=\frac{(x-\xi_1)\ \ldots\ (x-\xi_{i-1})(x-\xi_{i+1})\ \ldots\ (x-\xi_n)}{(\xi_i-\xi_1)\ \ldots\ (\xi_i-\xi_{i-1})(\xi_i-\xi_{i+1})\ \ldots\ (\xi_i-\xi_n)}\qquad (i=1,\ \ldots,\ n).$$

If we replace x by a variable ω of the field $F(\xi)$, the sum of the resulting fractions is equal to 1 for $\omega=\xi_i$, since then $e_{ii}=1$, $e_{kk}=0\,(k\neq i)$. Since the sum is a polynomial of degree

* Announced by the author, *Bulletin of the American Mathematical Society*, XII (1906), 442. The proof by Wedderburn, *Transactions of the American Mathematical Society*, XV (1914), 162–66, has been amplified here by the addition of (1)–(10).

$n-1$ in ω, which is equal to 1 for the n values $\xi_i (i=1, \ldots, n)$ of ω, it is identically equal to 1 (I, § 112). Hence

$$e_{11}+e_{22}+ \ldots + e_{nn}=1. \tag{4}$$

Since $e_{ii}e_{jj}(i\neq j)$ has the factor $\phi(x)$, it is zero. Multiplying (4) on the right by e_{ii}, we get (5_2):

$$e_{ii}e_{jj}=0 \quad (i\neq j), \qquad e_{ii}^2=e_{ii}. \tag{5}$$

From $xy=y\theta(x)$ and (2), we get

$$(x-\xi_i)y=y\{\theta(x)-\theta(\xi_{i+1})\}=y(x-\xi_{i+1})q_i,$$

in which the quotient q_i is a polynomial in x. By (3),

$$e_{11}=k\prod_{i=2}^{n}(x-\xi_i),$$

where k is independent of x. Hence

$$e_{11}y=yPQ(x), \qquad P=\prod_{i=2}^{n}(x-\xi_{i+1}), \qquad Q(x)=k\prod_{i=2}^{n}q_i$$

Writing j for $i+1$, we see that P is the product of the $x-\xi_j$ having $j\neq 2$, whence P is the product of e_{22} by a number of $F(\xi)$. By division,

$$Q(x)=(x-\xi_2)h(x)+r, \qquad r=Q(\xi_2).$$

But $P(x-\xi_2)=\phi(x)=0$. Hence

$$e_{11}y=yPr=ye_{22}c, \qquad e_{11}^2y=ye_{22}^2c^2,$$

whence $c^2=c$, $c=1$, and $e_{11}y=ye_{22}$.

If we permute $\xi_1, \ldots, \xi_n$ cyclically, also $e_{11}, \ldots, e_{nn}$ in (3) are permuted cyclically. Hence

$$e_{ii}y=ye_{i+1,\,i+1} \quad (i=1, \ldots, n), \tag{6}$$

with the agreement that $e_{n+j,\,n+j}$ denotes e_{jj}. By induction,

$$e_{ii}y^k=y^ke_{k+i,\,k+i}. \tag{7}$$

We employ the following new elements of D:

$$(8)\qquad e_{1i}=y^{i-1}e_{ii}\,,\qquad e_{i1}=\frac{1}{\gamma}\,y^{n+1-i}e_{11}\qquad (i=2,\ \ldots\ ,\ n).$$

Then, by (7),

$$e_{11}e_{1i}=y^{i-1}e_{ii}\cdot e_{ii}=e_{1i}\,,\qquad e_{1i}e_{i1}=\frac{1}{\gamma}y^{i-1}\cdot y^{n+1-i}e_{11}\cdot e_{11}=e_{11}\,,$$

$$e_{ii}e_{1i}=\frac{1}{\gamma}y^{n+1-i}\cdot y^{i-1}e_{ii}\cdot e_{ii}=e_{ii}\,,\qquad e_{i1}e_{11}=e_{i1}\,.$$

Introduce the elements $e_{rs}=e_{r1}e_{1s}$ for $r\neq 1$, $s\neq 1$, $r\neq s$. Hence

$$e_{ij}=e_{i1}e_{1j}\qquad (i,\ j=1,\ \ldots\ ,\ n),$$

$$e_{ij}e_{jk}=e_{i1}e_{1j}\cdot e_{j1}e_{1k}=e_{i1}\cdot e_{11}\cdot e_{1k}=e_{i1}e_{1k}=e_{ik}\,,$$

$$e_{ij}e_{kl}=e_{i1}e_{1j}\cdot e_{k1}e_{1l}=e_{i1}\cdot e_{1j}e_{jj}\cdot e_{kk}e_{k1}\cdot e_{1l}=0\qquad (j\neq k),$$

by (5_1). Hence the e_{ij} obey the multiplication table of the simple matric algebra (§ 51).

By (8), $\quad e_{12}=ye_{22}\,,\qquad \gamma e_{n1}=ye_{11}\,.\qquad$ For $1<i<n$,

$$e_{i,\,i+1}=e_{i1}e_{1,\,i+1}=\frac{1}{\gamma}\,y^{n+1-i}\cdot e_{11}y^{i}\cdot e_{i+1,\,i+1}=ye_{i+1,\,i+1}\,,$$

by (7). Summing and applying (4), we get

$$(9)\qquad y=e_{12}+e_{23}+e_{34}+\ \ldots\ .\ +e_{n-1,\,n}+\gamma e_{n1}\,.$$

As by the proof of (4), we have

$$(10)\qquad x=\xi_1e_{11}+\ \ldots\ .\ +\xi_ne_{nn}\,.$$

Since, conversely, the e_{ij} were expressed above as polynomials in x and y, this completes the proof that algebra A is the simple matric algebra having the n^2 basal units e_{ij}.

By (10), $x^s=\Sigma\xi_i^se_{ii}$. Multiply by a number a_s of the field $F(\xi)$ and sum as to s. Hence if $f(x)$ is any polynomial with coefficients in $F(\xi)$,

$$f(x)=\sum_{i=1}^{n} f(\xi_i)e_{ii}. \tag{11}$$

From (9) we find by induction that

$$y^r=\sum_{i=1}^{n-r} e_{i,r+i}+\gamma\sum_{j=1}^{r} e_{n-r+j,j}. \tag{12}$$

By way of check, note that $y^n=\gamma$. Hence

$$y^r f(x)=\sum_{i=1}^{n-r} f(\xi_{r+i})e_{i,r+i}+\gamma\sum_{j=1}^{r} f(\xi_j)e_{n-r+j,j}. \tag{13}$$

The matrix of (12) for $r<n$ is composed of zero elements except in two lines parallel to the main diagonal, that above the diagonal (on it if $r=0$) having $n-r$ elements 1 and that below it having r elements γ. Hence the determinant of the matrix (12) is $(-1)^{(n-r)r}\gamma^r$. The matrix of (13) is of the preceding type except that each element is now multiplied by a factor $f(\xi_s)$.

Hence in the matrix form of the general element

$$a=\sum_{r=0}^{n-1} y^r f_r(x)$$

of algebra A, each element below the main diagonal has the factor γ. For its determinant $|a|$ we therefore have

$$|a|_{\gamma=0}=f_0(\xi_1)\ \ldots\ f_0(\xi_n)=\text{norm}\, f_0(\xi_1), \tag{14}$$

We are now in a position to determine the conditions which γ must satisfy in order that D shall be a division algebra. For any given polynomials h_i in x with coefficients in D, we desire that

$$z=y^r+y^{r-1}h_1+\ \ldots\ +yh_{r-1}+h_r$$

shall have an inverse. Write

$$z_1 = y^{n-r} + y^{n-r-1}k_1 + \cdots + k_{n-r},$$

where the k_i are polynomials in x. Then

$$z_1 z = \gamma + y^{n-1}(h_1 + y^{-r}k_1 y^r) + y^{n-2}(h_2 + y^{1-r}k_1 y^{r-1}h_1 + y^{-r}k_2 y^r) + \cdots$$

The sums in parenthesis will be zero if

$$k_1 = -y^r h_1 y^{-r}, \quad k_2 = -y^r h_2 y^{-r} - y k_1 y^{-1} \cdot y^r h_1 y^{-r}, \cdots$$

These are polynomials in x with coefficients in F since

$$y^s f(x) y^{-s} = f[\theta^{n-s}(x)], \tag{15}$$

by (11) of § 47 with $r = n-s$. Hence we can determine $k_1, \cdots, k_{n-r}$ so that $z_1 z = z_2$, where z_2 is of degree $< r$ in y.

If z_2 has an inverse w, so that $wz_2 = 1$, then $wz_1 z = 1$ and z has the inverse wz_1. Let $y^t h(x)$ be the term of z_2 of highest degree in y. Then $t < r$ and h has an inverse l in the field $F(x)$ and hence in D. Thus z_2 will have an inverse if $z_2 l = y^t + \cdots$ has an inverse. The latter will have an inverse, by the argument just employed for z, if the next polynomial of degree $< t$ has an inverse.

It follows in this manner that z has an inverse unless we reach a pair of consecutive polynomials whose product does not involve y. Give them the foregoing notations, z_1, z. Then $z_1 z = \gamma + \delta$, where δ is independent of γ, since by (15) the coefficients of $k_1, k_2, \cdots$ of z_1 are independent of γ and since in forming the product $z_1 z$ we obtain the term $y^n = \gamma$ only once. For the moment, regard γ as a variable in F. If δ involves x, $\gamma + \delta$ is not zero and hence has an inverse in $F(x)$, so that z has an inverse in D. Hence let δ be a number of F.

Employing the matric forms of the z's, we have

$$z_1 z = (\gamma + \delta) I, \tag{16}$$

where I is the n-rowed unit matrix. By the remark below (13), the determinant $|z|$ of z is a polynomial in γ:

$$|z|=(-1)^{nr-r}\gamma^r+\ldots\ldots, \qquad |z_1|=(-1)^{r-nr}\gamma^{n-r}+\ldots\ldots.$$

Each is a factor of $(\gamma+\delta)^n$ by (16). Hence

$$|z|=(-1)^{nr-r}(\gamma+\delta)^r.$$

When $\gamma=0$, $|z|$ becomes norm h_r by (14). Hence

$$(-1)^{nr-r}\delta^r=\text{norm } h_r.$$

If $\gamma+\delta\neq 0$, z has an inverse. If $\gamma+\delta=0$, the last result shows that γ^r is the norm of $(-1)^r h_r$. This proves our theorem.

APPENDIX II

DETERMINATION* OF ALL DIVISION ALGEBRAS OF ORDER 9; MISCELLANEOUS GENERAL THEOREMS ON DIVISION ALGEBRAS

THEOREM 1. *If an algebra A of order α has a modulus e and contains a division sub-algebra B of order β whose modulus is also e, there exists a linear set C of order γ (of elements of A) such that $A=BC$, $\alpha=\beta\gamma$.*

For, if a_2 is an element of A which is not in B, the linear set $B+Ba_2$ is of order 2β, since otherwise there would exist elements b_1 and $b_2(b_2\neq 0)$ of B for which $b_1+b_2a_2=0$, whence $b_2^{-1}b_1+ea_2=0$, or $a_2=-b_2^{-1}b_1$, whereas a_2 is not in B. Then if $\alpha=2\beta$, we have $A=B(1, a_2)$ and the theorem is proved.

But if $\alpha>2\beta$, A contains an element a_3 which is not in $B+Ba_2$. The linear set $B+Ba_2+Ba_3$ is of order 3β, since otherwise B would contain elements b_1, b_2, $b_3\neq 0$ for which $b_1+b_2a_2+b_3a_3=0$, whence

$$a_3=-b_3^{-1}(b_1+b_2a_2)=b_4+b_5a_2,$$

* Amplification of the article by Wedderburn, *Transactions of the American Mathematical Society*, XXII (1921), 129–35.

whereas a_3 is not in $B+Ba_2$. Then if $\alpha=3\beta$, we have $A=B(1, a_2, a_3)$ and the theorem is proved. If $\alpha>3\beta$, we repeat the argument.

COROLLARY 1. *The order of a division algebra A is a multiple of the order of any sub-algbera.*

For, the sub-algebra is a division algebra with a modulus u. If e be that of A, then

$$u^2=u,\ ue=u,\qquad u(u-e)=0,\qquad u-e=0.$$

THEOREM 2. *Given a division algebra A over a non-modular field F, let the algebra B be composed of all those elements of A which are commutative with every element of A. We can find an extension F' of F such that the algebra A' over F', which has the same units as A, is the direct product of a simple matric algebra and the commutative algebra B' over F', which has the same units as B.*

For, by § 76, there exists a field F' obtained from F by adjoining a finite number of irrationalities $\xi_1, \xi_2, \ldots$, where $1, \xi_1, \xi_2, \ldots$ are linearly independent with respect to F, such that algebra A' over F' is a direct sum of simple matric algebras $A_1, \ldots, A_b$. Let e_i be the modulus of A_i. If $f=\Sigma f_i$, $g=\Sigma g_i$, where f_i and g_i are in A_i, and f is commutative with g, then

$$\Sigma f_ig_i=fg=gf=\Sigma g_if_i,\qquad f_ig_i=g_if_i.$$

By § 52 the products of e_i by numbers of F' are the only elements of A_i which are commutative with every element of A_i. Hence all those elements of A' which are commutative with every element of A' form an algebra B' with the basal units $e_1, \ldots, e_b$.

Since each e_i, and therefore also any element $y\neq 0$ of B', is a linear function of the basal units of A with coefficients in F', we may write $y=\Sigma\xi_ix_i$, where the x_i are elements, not all zero, of A, while $\xi_0=1$, and $\xi_1, \xi_2, \ldots$ are the foregoing irrationalities.

If x is any element of A (and hence in A'), $xy=yx$ by the definition of B'. Hence

$$o=xy-yx=\Sigma\xi_i(xx_i-x_ix).$$

Since each xx_i-x_ix is a linear function of the units of A with coefficients in F, and since the ξ_i are linearly independent with respect to F, we have $xx_i=x_ix$ for every i, and for every x in A. Hence the elements of the sub-algebra B (of A) generated by the x_i are commutative with every element of A. If x_0 is any element of A commutative with every element of A, then x_0 is in B, since x_0 is evidently commutative with every element of A' and hence is an element of B' of the special form $y=x_0+o\xi_1+o\xi_2+\ldots\ldots$ Thus B is the algebra defined in the theorem.

Since every element of B' is of the form $y=\Sigma\xi_ix_i$, B' has the same basal units as B, although the two algebras are over different fields F' and F.

The commutative division algebra B is a field. We may regard A as an algebra A_1 of order a/b over this field B. As above we extend the latter field to a field F_1 such that the algebra A_1' over F_1, with the same units as A_1, is a simple matric algebra or a direct sum of simple matric algebras. The latter alternative is excluded since otherwise B would not contain all elements commutative with every element of A. Since A_1' is a simple matric algebra, A' over F' is the direct product of B' and a simple matric algebra.

A division algebra A over F is called *normal* if the products of its modulus by numbers of F are the only elements of A which are commutative with every element of A, i.e., if the B of Theorem 2 is of order 1.

COROLLARY 2. *The order of any normal division algebra is a square.*

COROLLARY 3. *Any division algebra A whose order is the square of a prime p is either normal or is equivalent to a field.*

For, $p^2=bq^2$, where b is the order of its B. Hence $b=1$ or p^2. In the first case, A is normal. In the second case, $A=B$ is a commutative division algebra and hence is a field.

Polynomials over an algebra. Let A be any algebra having a modulus which will be designated by 1 Polynomials $a_0+a_1x+\ldots.+a_nx^n$ in an indeterminate x, having coefficients $a_0, \ldots., a_n$ in A, may be defined as in § 111, with the modification that, when ρ is an element of A and a denotes the set $(a_0, a_1, \ldots., a_n)$, $\rho a=(\rho a_0, \ldots., \rho a_n)$ and $a\rho=(a_0\rho, \ldots., a_n\rho)$ may now be distinct since A need not be a commutative algebra. However, $x=(0, 1)$ is commutative with every element of A and hence with the foregoing polynomial in x over A.

Two such polynomials are equal only when corresponding coefficients are equal. The sum and product of the two are found as in elementary algebra, provided care is taken in multiplication to preserve the order of factors belonging to A. Let

$$A=a_0\omega^m+\ldots.+a_m, \qquad B=b_0\omega^n+\ldots.+b_n \qquad (b_0\neq 0)$$

be two polynomials in the indeterminate ω over a division algebra D. If $n\leqq m$, we can determine unique polynomials Q and R in ω over D such that $A=QB+R$, where R is 0 or has a degree $<n$. In fact, we find

$$Q=a_0b_0^{-1}\omega^{m-n}+(a_1-a_0b_0^{-1}b_1)b_0^{-1}\omega^{m-n-1}+\ldots.$$

by the usual division process, taking care to multiply the divisor B on the left by the successive terms of Q. If $R\equiv 0$, A is said to have B as a right (right-hand) divisor and Q as a left divisor.

As in § 113, there exist greatest common right and left divisors C_1 and C_2 of A and B, and polynomials L_1, M_1, L_2, M_2 over D such that

$$L_1A+M_1B=C_1, \qquad AL_2+BM_2=C_2.$$

LEMMA. *If $A=BC$, B and C are polynomials in ω over a division algebra D, and if $\omega-x$ is a right divisor of A, but not of C, where x is in D, so that $C=Q(\omega-x)+R$, where $R\neq 0$ is independent of ω, then $\omega-y$ is a right divisor of B if $y=RxR^{-1}$ is the transform of x by R.*

For, by multiplying the expression for C by B on the left, we get

$$A=BQ(\omega-x)+BR.$$

Hence $\omega-x$ is a right divisor of $BR=Q'(\omega-x)$. Thus $B=Q'R^{-1}(\omega-y)$.

THEOREM 3. *If D is a normal division algebra over F, and if $\phi(\omega)=0$ is the equation of least degree p with coefficients in F which is satisfied by the element x_1 of D, there exist further elements $x_2, \ldots, x_p$ of D such that*

$$(1) \qquad \phi(\omega)\equiv(\omega-x_p)(\omega-x_{p-1})\ldots(\omega-x_2)(\omega-x_1).$$

Also $\phi(\omega)$ is the product of the same linear factors permuted cyclically.

Any element d of D is commutative with the coefficients (belonging to F) of $\phi(\omega)$ and also with ω. Since $\phi(x_1)=0$, $\phi(\omega)$ has the right divisor $C=\omega-x_1$. Transform each member of the identity $\phi(\omega)\equiv B(\omega-x_1)$ by d. We get

$$\phi(\omega)\equiv dBd^{-1}\cdot(\omega-dx_1d^{-1}),$$

so that, if t is any transform of x_1, then $\omega-t$ is a right divisor of $\phi(\omega)$.

Let x' be a transform of x_1 which is not equal to x_1. Write $\phi(\omega)=BC$. Since

$$C=\omega-x'+R, \qquad R=x'-x_1\neq 0,$$

we may apply the lemma with $x=x'$ and conclude that B has the right divisor $\omega-x_2$, where $x_2=Rx'R^{-1}$. Write $B=B'(\omega-x_2)$. Then

$$\phi(\omega)=B'C', \qquad C'=(\omega-x_2)(\omega-x_1).$$

Either we have (2) for $m=2$, or there exists a transform x'' of x_1 such that $\omega-x''$ is not a right divisor of $C'(\omega)$. The lemma shows that B' has the right divisor $\omega-x_3$, where x_3 is the transform of x'' by $C'(x'')\neq 0$. Continuing, we finally get

$$(2) \qquad \phi(\omega)=LM, \quad M\equiv(\omega-x_m)(\omega-x_{m-1})\ \ldots\ (\omega-x_2)(\omega-x_1),$$

where $m\leqq p$ and, if y is any transform of x_1, then $\omega-y$ is a right divisor of M. Write $M=\omega^m+\ \ldots\ +a_m$. Then

$$(3) \qquad y^m+a_1y^{m-1}+\ \ldots\ +a_m=0$$

for every transform y of x_1.

Suppose the a's are not all in F. Since D is normal, there is an element z of D which is not commutative with at least one a. Write $a_i'=za_iz^{-1}$. Transforming (3) by z, we get

$$(zyz^{-1})^m+a_1'(zyz^{-1})^{m-1}+\ \ldots\ +a_m'=0.$$

Hence every transform y of x_1 satisfies not only (3) but also

$$(4) \qquad y^m+a_1'y^{m-1}+\ \ldots\ +a_m'=0,$$

in which at least one coefficient differs from the corresponding coefficient of (3). Subtracting (3) from (4), we get an equation of degree $<m$ which is not identically zero and is satisfied by every transform of x_1:

$$y^q+\beta_1y^{q-1}+\ \ldots\ +\beta_q=0.$$

If the β's are not all in F, the degree can be reduced again by the preceding process. We finally obtain an equation with coefficients in F which is satisfied by every transform of x_1 and hence by x_1 itself. But of such equations, $\phi(\omega)=0$ is the one of least degree p. Hence $m\geqq p$. Thus $m=p$ and $\phi(\omega)=M$. This proves (1).

Finally, we can permute the linear factors of (1) cyclically if $p>1$. Write $\phi\equiv P(\omega-x_1)$. The unique division process yields $\phi\equiv Q(\omega-x_1)$, where Q is a polynomial in ω and x_1 with coefficients in F. Hence $Q\equiv P$ is commutative with $\omega-x_1$, whence $\phi\equiv(\omega-x_1)P$, as desired.

THEOREM 4. *If A is an algebra over a non-modular field F and if y is an element for which the rank equation of A has no multiple roots, then any element of A which is commutative with y is a polynomial in y with coefficients in F.*

For, let x be the general element $x=\Sigma\xi_i e_i$ of an algebra A over a non-modular field F. Let the rank equation of A be

$$f(x,\xi)=a_0(\xi)x^r+a_1(\xi)x^{r-1}+\ \ldots\ +a_r(\xi)=0,$$

where ξ denotes the set of co-ordinates $\xi_1, \ldots, \xi_n$ of x. Let $y=\Sigma\eta_i e_i$ be a particular element of A such that $f(y,\eta)=0$ has no multiple roots. We seek the elements x which are commutative with y.

Let λ be a variable in F. Then $f(y+\lambda x,\ \eta+\lambda\xi)=0$. The coefficient of each power of λ in its expansion must be zero. If we write

$$a_i(\eta+\lambda\xi)=a_i(\eta)+\lambda a_{i1}(\eta,\ \xi)+\lambda^2 a_{i2}(\eta,\ \xi)+\ \ldots\ ,$$

and equate to zero the coefficient of λ^1 in f, we get

$$f'(y,\eta)x+\sum_{i=0}^{r}a_{i1}(\eta,\ \xi)y^{r-i}=0,$$

where f' denotes the derivative with respect to y and is not zero. Hence f' has an inverse which is a polynomial in y (§ 84).

THEOREM 5. *Every normal division algebra D of order 9 over a non-modular field F is generated by elements x and y such that $xy=y\theta(x)$, $y^3=\gamma$, where γ and the coefficients of the*

polynomial $\theta(x)$ belong to F, while x, $\theta(x)$ and $\theta^2(x)=\theta[\theta(x)]$ are the roots of a cubic equation irreducible in F.*

For, by Theorem 2 in which B is now of order 1, D is a simple matric algebra over an extended field. Hence the rank equation of D is of degree 3 (§ 71). Thus the equation of lowest degree with coefficients in F satisfied by an element x_1 not in F is of the form†

$$\phi(\omega)\equiv\omega^3+a_1\omega^2+a_2\omega+a_3=0. \tag{5}$$

i) If D contains an element x_1 not in F which is commutative with a transform $t=y^{-1}x_1y$ of x_1 ($t\neq x_1$), Theorem 4 shows that t is a polynomial $\theta(x_1)$ in x_1 with coefficients in F. By the foregoing, $\omega-t$ is a right divisor of $\phi(\omega)$ and hence t is a root of (5). Since the latter is irreducible, and has a root x_1 in common with $\phi(t)\equiv\phi[\theta(x_1)]=0$, all of its roots satisfy the latter, by Theorem 7 of § 84, whence $\theta^2(x_1)$ is a root of (5) and $\theta^3(x_1)$ is equal to the root x_1. By the two expressions for t,

$$x_1y=y\theta(x_1),\qquad x_1y^2=y^2\theta^2(x_1),\qquad x_1y^3=y^3\theta^3(x_1)=y^3x_1,$$

whence y^3 is commutative with x_1 and by Theorem 4 is expressible as a polynomial in x_1:

$$y^3=\lambda x_1^2+\mu x_1+\nu,$$

with λ, μ, ν in F. If λ and μ are not both zero, y^3 is not in F and its adjunction extends F to the algebra $(1, x_1, x_1^2)$ of order 3 over F. But y^3 extends F to a sub-algebra of $(1, y, y^2)$ and hence to the latter itself. Thus y is a polynomial in x_1 and hence is commutative with x_1, whereas y transforms x_1 into $t\neq x_1$. This contradiction proves that $y^3=\nu$. Hence Theorem 5 is true for case (i).

* By (10), § 47. The algebra is of the type treated in §§ 47, 48.

† By Corollary 1, it is not of degree 2.

ii) Let D contain an element x_1 which is not commutative with any of its transforms other than x_1 itself. By Theorem 3 there exist transforms x_2 and x_3 of x_1 such that

$$\phi(\omega)\equiv(\omega-x_3)(\omega-x_2)(\omega-x_1), \tag{6}$$

in which the three factors may be permuted cyclically. We proceed as in the proof of Theorem 3 with now

$$x'=(x_1-x_3)x_1(x_1-x_3)^{-1},$$

which is distinct from x_1, since otherwise $x_1x_3=x_3x_1$, contrary to the hypothesis on x_1. Hence

$$x_2=Rx'R^{-1}=Sx_1S^{-1}, \qquad S=(x'-x_1)(x_1-x_3),$$
$$S=x'(x_1-x_3)-x_1(x_1-x_3)=(x_1-x_3)x_1-x_1(x_1-x_3),$$
$$x_2=(x_1x_3-x_3x_1)x_1(x_1x_3-x_3x_1)^{-1}. \tag{7}$$

Comparing (5) with (6), we have

$$x_3x_2+x_2x_1+x_3x_1=a_2.$$

Permuting x_3, x_2, x_1 cyclically, we get

$$x_2x_1+x_1x_3+x_2x_3=a_2, \qquad x_1x_3+x_3x_2+x_1x_2=a_2.$$

By subtraction,

$$y\equiv x_2x_1-x_1x_2=x_1x_3-x_3x_1=x_3x_2-x_2x_3.$$

Then (7) becomes

$$x_2=yx_1y^{-1}. \tag{8}$$

Permuting x_3, x_2, x_1 cyclically, we see that the three preceding values of y are permuted cyclically. Hence (8) gives

$$x_1=yx_3y^{-1}, \quad x_3=yx_2y^{-1}=y^2x_1y^{-2}, \quad x_1=y^3x_1y^{-3}, \tag{9}$$

whence y^3 is commutative with x_1 and by Theorem 4 is expressible as a polynomial in x_1. As shown above, either y

itself is commutative with x_1, in contradiction with (8), or y^3 is an element of F.

If any transform (other than y) of y is commutative with y, we have case (i). If no such transform is commutative with y, we take y as the x_1 employed at the beginning of case (ii). Thus our discussion of case (ii) holds with the simplification $x_1^3=\gamma$, where γ is in F. Write

$$z_1=x_1y, \qquad z_2=x_1z_1x_1^{-1}=x_1^2yx_1^{-1}. \tag{10}$$

Then

$$z_1z_2-z_2z_1=x_1yx_1^2yx_1^{-1}-x_1^2y^2=x_1(yx_1^2y-x_1y^2x_1)x_1^{-1}.$$

Since (6) is now identical with $\omega^3-\gamma$, $x_3^3=\gamma=x_2x_1x_3$, whence

$$0=x_3^2-x_2x_1=y^2x_1^2y^{-2}-yx_1y^{-1}\cdot x_1=y(yx_1^2y-x_1y^2x_1)/\nu,$$

by (8), (9), and $y^3=\nu$. Hence $z_1z_2-z_2z_1=0$, so that z_1 is a polynomial $\theta(z_2)$ with coefficients in F. By (10),

$$z_2x_1=x_1z_1=x_1\theta(z_2), \qquad x_1^3=\gamma.$$

Replacing z_2 by x, and x_1 by y, we obtain Theorem 5.

Hence by Corollary 3 every division algebra of order 9 is either a field or is of the type in Theorem 5.

APPENDIX III

STATEMENT OF FURTHER RESULTS AND UNSOLVED PROBLEMS

1. If $A_1, \ldots, A_s$ is a series of algebras such that each A_r is a maximal invariant proper sub-algebra of its predecessor A_{r-1}, while A_s is simple, the series is called a *series of composition* of A_1. The series of simple algebras A_1-A_2, $A_2-A_3, \ldots, A_{s-1}-A_s$, A_s is called a *series of differences* of A_1.

Algebra (1) in § 20 has the series of composition $A=(u_1, u_2, u_3)$, (u_1, u_2), (u_1), as well as that derived by any per-

mutation of 1, 2, 3. For each of these six series of composition of A, the series of difference algebras is composed of three algebras of order 1, each generated by an idempotent element. Since all such algebras of order 1 are equivalent, this illustrates the theorem* that two series of differences of the same algebra contain the same number of algebras, and the algebras of one series are equivalent to those of the other series when properly rearranged. If A is an algebra of index a and if the order n of A exceeds that of A^a by r, each series of differences of A can be so arranged that the first r terms are zero algebras of order 1. Hence, if $a>1$, A has an invariant sub-algebra of order $n-1$.

2. An associative algebra A with a modulus ϵ over a field F is reducible† with respect to F if and only if it contains an idempotent element $\neq\epsilon$ which is commutative with every element of A.

3. If‡ an associative algebra A has no modulus, but contains an invariant sub-algebra having a modulus, then A can be expressed in one and only one way as a direct sum of an algebra B with a modulus and an algebra C which has no modulus and no invariant sub-algebra which has a modulus.

4. The author§ has recently found all associative algebras with a modulus of order n and rank n or 2 over any non-modular field, and deduced all algebras of orders 2, 3, 4. If A is of order and rank n, it contains an element x such that $1, x, x^2, \ldots, x^{n-1}$ are dependent, while x is a root of an equation $f(\omega)=0$ of degree n with coefficients in F.

* Wedderburn, *Proceedings of the London Mathematical Society*, Series 2, Vol. VI (1907), pp. 83–84, 89.

† Scheffers, *Mathematische Annalen*, XXXIX (1891), 319; *Linear Algebras*, pp. 26–27.

‡ Communicated by Wedderburn. B is an invariant sub-algebra which has a modulus and is contained in no other invariant sub-algebra having a modulus. Then $A=B\oplus C$ by § 22.

§ *Proceedings of the London Mathematical Society*, 1923.

Then A is irreducible with respect to F if and only if $f(\omega)$ is irreducible or is a power of a polynomial irreducible in F.

5. Consider* algebra C in which multiplication is defined by

$$(q+Qe)(r+Re)=t+Te, \quad t=qr-R'Q, \quad T=Rq+Qr',$$

where q, Q, r, R are any real quaternions, and r', R' are the conjugates of r, R. Taking $r=q'$, $R=-Q$, we get

$$N(q+Qe)\equiv(q+Qe)(q'-Qe)=qq'+QQ'.$$

The norm of a product is the product of the norms of the factors. Each of the two kinds of division except by zero is always possible and unique, so that C is a division algebra; it is not associative. The author† has discussed the arithmetic of C at length.

6. If‡ a division algebra A over F contains a normal subalgebra B, A can be expressed as the direct product of B and another algebra C over F. Further results on division algebras have been obtained by the author§ and O. C. Hazlett.|| Every associative division algebra over a finite field is a field.¶

* Dickson, *Transactions of the American Mathematical Society*, XIII (1912), 72; *Annals of Mathematics*, XX (1919), 155–71, 297; *Linear Algebras*, p. 15. An equivalent real algebra of order 8 had been given by Cayley.

† *Journal de Mathématiques*, Sér. 9, Tome II (1923).

‡ Wedderburn, *Transactions of the American Mathematical Society*, XXII (1921), 132. The proof is by the corollary to Theorem 2 in *Linear Algebras*, pp. 28, 29.

§ *Transactions of the American Mathematical Society*, VII (1906), 370, 514; XIII (1912), 59; XV (1914), 39; *Bulletin of the American Mathematical Society*, XIV (1907–8), 160; *Göttinger Nachrichten* (1905), pp. 358–93; *Linear Algebras*, pp. 69, 71.

|| *Transactions of the American Mathematical Society*, XVIII (1917), 167–76.

¶ Wedderburn, *op. cit.*, VI (1905), 349; Dickson, *Göttinger Nachrichten* (1905), p. 381.

7. Invariantive characterizations of algebras and certain vector covariants of them have been given by Hazlett* and MacDuffee†. The author‡ deduced the algebra of quaternions from relations between algebras and continuous groups.

8. There are papers§ dealing with the relations between linear algebras and finite groups, and others dealing with analytic functions of hypercomplex numbers.

9. Among the unsolved problems are the determination of all division algebras, the classification of nilpotent algebras, the discovery of relations between an algebra and its maximal nilpotent invariant sub-algebra (cf. §§ 101–3 for the case of complex algebras), theory of non-associative algebras, theory of ideals in the arithmetic of a division algebra, and the extension to algebras of the whole theory of algebraic numbers.

* *Annals of Mathematics*, XVI (1914), 1–6; XVIII (1916), 81–98; *Transactions of the American Mathematical Society*, XIX (1918), 408–20.

† *Transactions of the American Mathematical Society*, XXIII (1922), 135–50.

‡ *Bulletin of the American Mathematical Society*, XXII (1915), 53–61; *Proceedings of the National Academy of Sciences*, VII (1921), 109–14.

§ *Linear Algebras*, pp. 63, 73; or *Encyclopédie des Sciences Mathématiques*, Tome I, Vol. I (1908), pp. 436, 441.

INDEX

[Numbers refer to pages]

PRINTED IN THE U.S.A